Cellebrite May 2021 Manuals for Touch2 UFED, 4PC UFED

1. Notice

This book was produced in EPUB format by the Internet Archive.

The book pages were scanned and converted to EPUB format automatically. This process relies on optical character recognition, and is somewhat susceptible to errors. The book may not offer the correct reading sequence, and there may be weird characters, non-words, and incorrect guesses at structure. Some page numbers and headers or footers may remain from the scanned page. The process which identifies images might have found stray marks on the page which are not actually images from the book. The hidden page numbering which may be available to your ereader corresponds to the numbered pages in the print edition, but is not an exact match; page numbers will increment at the same rate as the corresponding print edition, but we may have started numbering before the print book's visible page numbers. The Internet Archive is working to improve the scanning process and resulting books, but in the meantime, we hope that this book will be useful to you.

The Internet Archive was founded in 1996 to build an Internet library and to promote universal access to all knowledge. The Archive's purposes include offering permanent access for researchers, historians, scholars, people with disabilities, and the general public to historical collections that exist in digital format. The Internet Archive includes texts, audio, moving images, and software as well as archived web pages, and provides specialized services for information access for the blind and other persons with disabilities.

Created with hocr-to-epub (v.1.0.0)

@) Cellebrite UFED and Responder Performing extractions May 2021 | Version 7.45 ‘:: Cellebrite

Copyright © 2021 Cellebrite DI Ltd. All rights reserved. This document is delivered subject to the following conditions and restrictions: » This document contains proprietary information belonging to Cellebrite DI Ltd. Such information is supplied solely for the purpose of assisting explicitly and properly authorized users of the Cellebrite UFED/Responder. » No part of this content may be used for any other purpose, disclosed to any person or firm, or reproduced by any means, electronic or mechanical, without the express prior written permission of Cellebrite Ltd. » The text and graphics are for the purpose of illustration and reference only. The specifications on which they are based are subject to change without notice. » Information in this document is subject to change without notice. Corporate and individual names and data used in examples herein are fictitious unless otherwise noted.

The text on this page is estimated to be only 41.71% accurate

Te a 7 WN oy SSN SUNG STS gaa gat sh oar a a al eh ae Sa 8 1.2. Extraction typ@s oso o ce ee eee eee eee see eee eee 9 Mes Se a a gp 10 1.3.1. Cellebrite UFED Device Adapter with USB 3.0 __. i Te MTEL 2M PCD oo ei ee Se Sls 13 1.3.3. Using cables and tips _-_____ ee. 13 | BUGIS WAVICCS ets ee ee eee 14].0. Gellebrite YouTube-channel .--. 0 14 2 JPOGI Gal: BxPeClon 2220 ese ee sce see ees 15 2.1. Advanced logical Android extraction _____ 16 Ze ls Whe eriacied Cala Wer 22 5.6o el oe Seo Le ee oes, 16 2.2. Aavanced logical (0S BXUaCHON Wo Socata eS eee eee ees, l? 2.2.1. Encrypted iTunes backup _____-_ 20 Pe OVE ee eUN 2 apc eieeetet, ate e eee, 21 2.4. Logical extraction via Bluetooth _____ ee. 24 O. PaSSWOPG ExURACUON ao a ee a 29 a. etree hing Ihe WEerlOC, = foe a 29 3.1.1. The extracted passwords folder _____ ee. oe 3.2. Disabling or re-enabling the user lock _____-_---_-_------- 3° Gd. REMOVING THE SGreet LOCK ano ee eee 39 4. File system extraction _____-_-_-_- ee 38 Contents

4.1. Performing a file system extraction _____-_ 38 4.1.1. The file system extraction folder _____ 40 4.2. Android backup ___--_ 4] Ue, Wye MUPAGUC OA GS 3s ake ee tee Se ee eee eee 44 4.3. Android backup APK downgrade _____-_- 45 4.3.1. Android backup APK downgrade - Manual installation _-_____. 90 de Vee EWG Wat Soto je te Sy) eA Ne NG eC WMO, heat See ee, 3 4.5. Selective file system extraction _____-_ 56 By PRysital SxtraCu Ot. 2. 59 6.1. Performing a physical extraction _-_--_- 60 6.1.1. The Physieal extraction older a 62 Ge AUB WOOO 203205222 ee i a eee 63 Geo USING OO FUG Or patos oa 65 6.3) |, GemenCinouell 2... oe loa oe ee oo ee 13 6.3.2. Errors and notifications _-- 79 64. Bootloader (RW tlashing) 2. ee ee 82 oom Bc or g's e119 (966/610) Ma (c= 6) =) ee a ee et ae ee ae ee ne eee 85 6.6. Forensic recovery partition _---- 87 ics AUN ce EY te i i 71 7. Capture images and screenshots _____--_-- 95 7.1. The Cellebrite UFED camera _____-_____-_- 99 7.2. Gapturing images... 96

The text on this page is estimated to be only 38.83% accurate

7 od GaRTUNING SCreGNSNOlS.. jase ee ee ee 100 oan Oye: er.) 9) | ge ee ee ee eae eee 102 8.1. Performing a Chat capture by application ___. 102 8.2. Performing a Chat capture in Generic mode _____ 104 9. SIM card functionality _____-_-_---ee eee. 107 Nas OM HRA, CARSON a ca gh et as ha lee alte Loe 9.1.1. Performing SIM data extraction _____ 107 gov otek Te ac Renee eR ten oY a SN ere OR nN La 72. ining an existing. SIM Cara: 2c oc ee ee eo el 111 V2e2, Envering- ol) Gate Mmanulaluy 220 oo tee el ee ek 114 V2.0. Greening @ OSM Test SNM 6. Sep ee 118 10. Drone extractions _____-_---- ____---------- TW? TT Device tools: soca ce esc tea eeeceeeshees Gecetea canada cneteaueecaenct 122 hele ACtiveare Tomiomtinlog ac.) jet gee ee ee ee ee ee A ee 124 WieZeAndrord Debug CGnSOle a2 ees ee i sy et Se 124 1.3. Bluetooth scan __--- 126 1.4. Disable iTunes encryption password ___-- 126 TV pia ESEUE PAV GI SCO IY VOI C t heateettaree l 127 Tse SEUE IMU TOT CS GUN je cr ea Sh ee a ee, 127 Mile alee ECMO e as tes Se 2 ee ee ee ee ae 8. Flash Cable 500 Firmware _____- Zi NO aE 1 | = 1 (=) ig) enn np Tv ee 128 11.10. Nokia WP8 recovery tool _-____ 128 5 iF Cellebrite

The text on this page is estimated to be only 44.33% accurate

11.11. Remove Android extraction files __.. 128 11.12. Samsung Exynos Recovery ..0 22 128 11.13. Saved APKs from APK downgrade ___-_-- 129 ale. Switch te OMA Omlineimode: .- 522-55 5o562 5c e eases a ees 130 o. Uninstall Windows mobile cent 2 ee ee Pe a 1 AEE C7 Uo = < |! eee a OPN OE a ee REE SRE Cee ae eS Ree PE 132 13. Index __---___--__---- ee 133 Contents 6

1. Overview Cellebrite UFED/Responder is a new generation solution that empowers law enforcement, military, intelligence, personnel to capture critical forensic evidence from Android and iOS mobile devices. Cellebrite UFED/Responder enables you to: » »> » »> » Perform physical, file system, and logical extraction of device data and passwords. Capabilities may vary, based on the Cellebrite UFED/Responder product purchased Cellebrite UFED/Responder Logical or Cellebrite UFED/Responder Ultimate. Extract vital data such as call logs, phonebook entries, text messages [SMS], pictures, videos, audio files, ESN IMEI, ICCID and IMSI information and more, from a wide range of mobile devices. Extract data from the widest selection of operating systems, such as Apple i0S, Blackberry, Android, Symbian, Microsoft Mobile, and Palm OS. Clone the SIM ID, which allows you to extract phone data while preventing the mobile device from connecting to the network. It can also help if the SIM card is missing. Extract the data from a mobile device either by a cable based connection [serial or USB] or a Bluetooth wireless connection. The tips and cable kit consists of four master cables and various tips. This manual ts also relevant for Cellebrite Responder users.

1.1. System requirements Windows compatible PC with Intel 15 or compatible running at 1.9 GHz or EY higher Microsoft Windows 10, 64-bit Operating Microsoft Windows 8.x, 64-bit system Microsoft Windows 7, 64-bit Microsoft Windows 7 Boot Camp on MAC Recommended Minimum Memory (RAM) 16 GB 46GB Space : 1.5 GB of free disk space for installation requirements Additional ; Microsoft .Net version 4.5 or later requirements If you intend to activate the application using a hardware license key Permissions (dongle) provided by Cellebrite, you must have administrative rights over the computer. This specification is for a PC running both Cellebrite UFED/Responder and the Physical Analyzer application as the decoding operations of Physical Analyzer require the higher specification. For a standalone PC running Cellebrite UFED/Responder an ATOM based chipset [or equivalent) is sufficient. Chapter 1: 8

1.2. Extraction types Cellebrite UFED/Responder includes a range of data extraction types. S® The available extractions may vary, based on the type of product =) vel yp p purchased; the Cellebrite UFED/Responder Logical or the Cellebrite UFED/ Responder Ultimate product. Table 1-1: Functionalities of the Cellebrite UFED/Responder products Cellebrite UFED/Responder | Cellebrite UFED/Responder Logical Ultimate Functionality Logical Extraction Yes SIM Data Extraction Yes Yes Password Extraction Yes Yes Clone SIM Yes Yes File System Extraction Not available Yes Physical Extraction Not available Yes ae atte Dpuolas ee Chat capture Yes Yes The extraction types are: » Logical extraction: Extracts user data from a mobile device (SMS, call logs, pictures, phonebook, videos, audio, certain application data, and more). Quickest extraction method but least amount of data. >» SIM card extraction: Extracts data from a SIM or USIM card. » File system extraction: Extracts files embedded in the memory of a mobile device. Retrieve the artifacts within a Logical extraction, in addition to hidden system files, databases and other files which were not visible within a logical extraction. »» Password extractions: Unlocks and displays passwords from a source mobile device. » Clone SIM: Copies a SIM ID from one SIM card to another SIM card or to a Cellebrite UFED SIM ID Access Card. >» Physical extraction: Extracts a physical bit-for-bit image of the flash memory of a device, including the unallocated space using advanced methods. Unallocated space is the area

of the flash memory that is no longer tracked by the file system, which may contain images, videos, files, and more. >» Capture images and screenshots: Take pictures or videos of a device using the Cellebrite UFED camera. You can also capture internal screenshots directly from the connected device. » Chat capture: Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data. 1.3. Accessories The Cellebrite UFED kit includes connection cables and tips. These are used in order to connect mobile devices to Cellebrite UFED. Figure: Cellebrite UFED Cables and tips The Cellebrite UFED Ultimate kit contains tips and cables for logical, file system, and physical extractions. The Cellebrite UFED Logical kit contains tips and cables for Logical Extraction only. Chapter 1: 10 ee

1.3.1. Cellebrite UFED Device Adapter with USB 3.0 The Cellebrite UFED kit contains a device adapter that attaches to your PC’s USB ports. Each connector has a LED that indicates availability during an extraction and blinks to indicate where to connect the source device. In addition, there are LEDs for power and Bluetooth. Depending on when you received your kit, there are two types of device adapters: Cellebrite UFED Device Adapter with USB 3.0 (latest version] and Cellebrite UFED Device Adapter with USB 2.0 [previous version]. This document provides more information on the Cellebrite UFED Device Adapter with USB 3.0. This manual ts also relevant for Cellebrite Responder users. Some devices can be extracted only by using the Cellebrite UFED Device Adapter.

This device adapter has the following connectors: » GPIO port [for future use] » USB 3.0 port » RJ45 port » DC In power supply (Input 5.3V 3.7A) » 2 USB connection cables labeled POWER and DATA. For information on the specifications, refer to the Overview Guide. To connect the Cellebrite UFED Device Adapter with USB 3.0: 1. First connect the DATA cable to a USB port on the computer. 2. Then connect the POWER cable to a second USB port on the computer. S 7 m - oO is) om < @ > roe = =] Use the following procedure, if the computer is mounted ina difficult to access or distant location. To connect the Cellebrite UFED Device Adapter with USB 3.0 using extension cables: 1. Connect the Active Extension cable to the DATA connection cable. Refer to the Overview Guide. 2. Connect the other end of this extension cable to a USB port on the PC. 3. Connect a standard USB extension cable to the POWER connection cable. 4. Connect the other end of this extension cable to a USB port on the PC. Chapter 1:

1.3.1.0.1. Using the External power supply The external power supply is NOT required for the smooth operation of the Cellebrite UFED Device Adapter V3, but is provided for those cases where additional power output is required. The external power supply provides an output of approximately 5.3V 2.7A. 1.3.2. Multi SIM Adapter A Multi SIM Adapter supports Micro, Nano and standard SIM cards. It is recommended to connect the Multi SIM Adapter to an available USB port on your computer, not to the USB port on the Cellebrite UFED Device Adapter. 1.3.3. Using cables and tips The cables and tips include various adapter cables {the number of cables depends on the Cellebrite UFED product and kit purchased). Each cable has a letter and name for example: A Adapter - USB. Figure: Single cable For easy recognition, the tips are color coded and numbered; the color represents the vendor. FS = Figure: Cellebrite UFED tip [example]

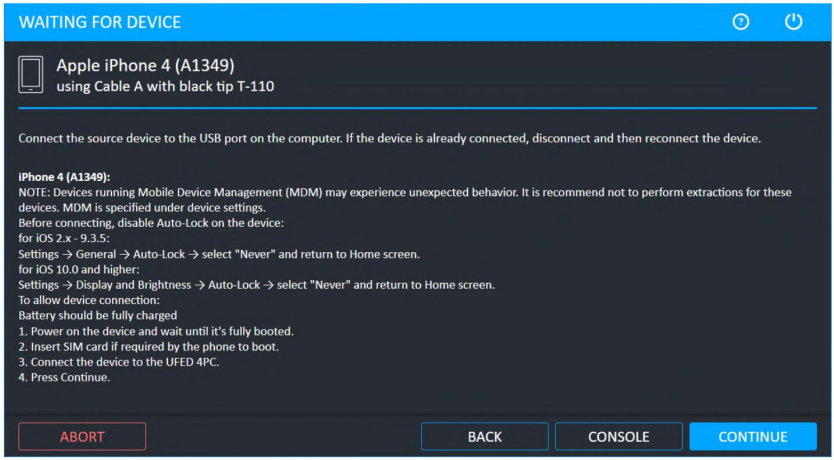
It is recommended to connect the Multi SIM Adapter to an available USB port on your computer, not to the USB port on the Cellebrite UFED Device Adapter.

Before each extraction, the required cable and tip number and color is specified in the Source area of the Select Content Types screen. 1.4. Supported devices To find out which mobile devices are supported in Cellebrite UFED and which data extraction capabilities are available for every mobile device use one of the following: 1. The Cellebrite UFED <version no> Supported Phone List file is delivered with every Cellebrite UFED software version update. The Microsoft Excel file contains two worksheets: The Cellebrite UFED Logical sheet lists the mobile devices supported for logical extraction. The Cellebrite UFED Physical sheet lists the mobile devices supported for physical, file system, and password extractions. 2. UFED Phone Detective (devices supported for logical extraction only). 3. Cellebrite UFED Supported Devices document in MyCellebrite. 1.5. Cellebrite YouTube channel For your convenience, a selection of useful videos demonstrating typical workflows and common procedures are available at youtube.com/cellebriteufed. Chapter 1: 14

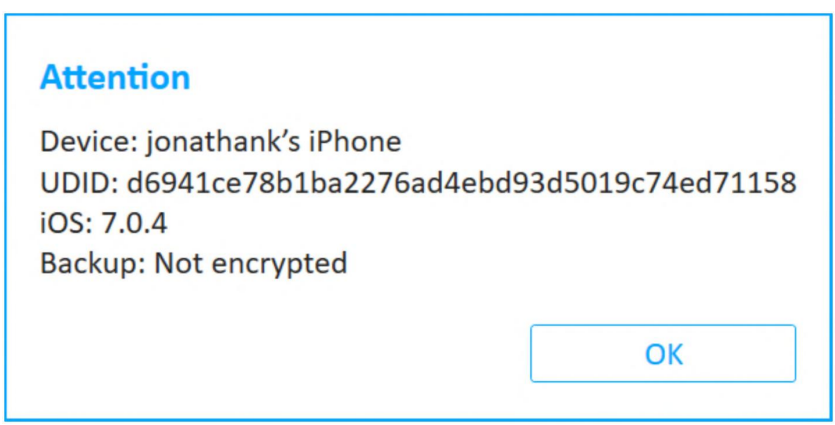
2. Logical extraction The Logical Extraction function enables you to extract various types of data, such as call logs, phonebook records, SMS text messages, calendar events, and multimedia files limages, videos, etc.). Save the extracted data from the source device to your PC or to a removable storage device, as desired. In most cases, a logical extraction is not possible for locked devices. A logical extraction can also be used to extract data from many Android, BlackBerry, 10S, and Windows Phone apps. For an updated list of supported apps and versions for each platform go to Help > Supported Apps in Physical/Logical Analyzer. Data extracted from these apps can be analyzed using Physical/Logical Analyzer (although the data is not included in UFED HTML and XML reports). The available types of extracted data may vary depending on the source device manufacturer and model. The supported data types are listed in the UFED Phone Detective or within the UFED Supported Devices. Logical extraction includes the following: Advanced logical Android extraction (on the next page) Advanced logical iOS extraction (on page 17) Logical (Partial) [on page 21) Logical extraction via Bluetooth [on page 24)

2.1. Advanced logical Android extraction The following procedure explains the Advanced logical extraction process for an example device. The procedure may vary depending on the selected device. This section shows only one of the many extraction types that can be performed. 2.1.1. The extracted data folder At the end of the data extraction process, the extracted data is saved in the location you selected. The extracted data folder is named “UFED" with the selected device name, the IMEI/MEID info. and the extraction date. For example, “UFED Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 2014_11_10 (0001)" The extracted data folder contains: » Multimedia files folders named Audio, Images, Ringtones, and Video folders, containing each of the respective type of media files. » Phone extraction report files in HTML and XML formats. [One HTML report per content type} » Cellebrite UFED Manager files of the extracted calls log (*.clog), phonebook [(*.pbb}, SMS messages [*.sms], and calendar (*.cal) Email(*.Email), MMS(*.MMS] and IM[*.IM] data. » UFD file. UFED Manager files are generated only for data types that contain items. The XML file can be viewed by both Logical Analyzer and Physical Analyzer. Chapter 2: 16

2.2. Advanced logical iOS extraction The Advanced logical extraction uses other extraction protocols and can potentially extract additional data compared to the standard logical extraction. Advanced logical extractions can be used to extract data from Android or iOS operating systems. The following example shows an Advanced logical iOS extraction. To perform an advanced logical iOS extraction: 1. Click Mobile device and identify the device. 2. Click Advanced Logical. For information on using optional timeframe and party filters, refer to the Overview Guide. The following window appears. WAITING FOR DEVICE Apple iPhone 4 (A1349) using Cable A with black tip T-110 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. iPhone 4 (A1349): NOTE: Devices running Mobile Device Management (MDM) may experience unexpected behavior. It is recommend not to perform extractions for these devices. MDM is specified under device settings. Before connecting, disable Auto-Lock on the device: for iOS 2.x - 9.3.5: Settings > General > Auto-Lock > select "Never" and return to Home screen. for iOS 10.0 and higher: Settings > Display and Brightness > Auto-Lock > select "Never" and return to Home screen. To allow device connection: Battery should be fully charged 1. Power on the device and wait until it's fully booted. 2. Insert SIM card if required by the phone to boot. 3. Connect the device to the UFED 4PC. 4. Press Continue. CONSOLE CONTINUE 3. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device. 4. Click Continue. The following window appears. Source Instructions Please unlock the device and choose ‘Trust’ when the trust message displays. Note: Devices with iOS 11 may also require the device password. If the password is requested enter it to proceed with the extraction. 5. Unlock the device and select Trust on the device. The following window appears.


WAITING FOR DEVICE
Apple iPhone 4 (A1349)
using Cable A with black tip T-110
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
iPhone 4 (A1349):
NOTE: Devices running Mobile Device Management (MDM) may experience unexpected behavior. It is recommend not to perform extractions for these devices. MDM is specified under device settings.
Before connecting, disable Auto-Lock on the device:
for iOS 2.x - 9.3.5:
Settings -> General -> Auto-Lock -> select "Never" and return to Home screen.
for iOS 10.0 and higher:
Settings -> Display and Brightness -> Auto-Lock -> select "Never" and return to Home screen.
To allow device connection:
Battery should be fully charged
1. Power on the device and wait until it's fully booted.
2. Insert SIM card if required by the phone to boot.
3. Connect the device to the UFED 4PC.
4. Press Continue.
ABORT
BACK
CONSOLE
CONTINUE

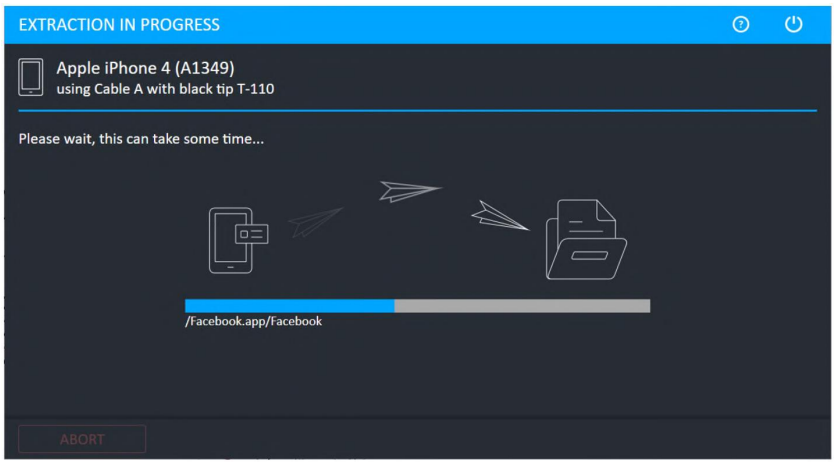
Attention Device: jonathank’s iPhone UDID: d6941ce78b1ba2276ad4ebd93d5019c74ed71158 iOS: 7.0.4 Backup: Not encrypted 6. This window displays the device name, UDID, iOS version, and whether the backup is encrypted. Click OK. If the iTunes backup is not encrypted, the following message about data encryption appears. If the iTunes backup Is encrypted, see Encrypted iTunes backup (on page 20). Attention To extract user credentials from an iOS device, backup encryption should be enabled (encryption is automatically disabled at the end of a successful extraction). Enable backup encryption? (UFED will temporary set the password to "1234",) 7. In the Attention window click Yes to enable backup encryption with the ability to extract additional information from the device, or click No if you do not require the additional information. The following window appears. There is an option to encrypt the 10S file. This additional layer of security allows 10S to include more sensitive information not found on a standard iCloud or iTunes backup file, including login details for apps and email accounts and other services that may be in use. You can extract an iOS keychain [user credentials} using this extraction method. At the end of the extraction, the encryption will automatically be reset. You can view the user credentials under the Passwords tree item in Physical Analyzer. If the extraction was stopped and the device remains encrypted, see Disable iTunes encryption password [on page 126). Chapter 2: 18



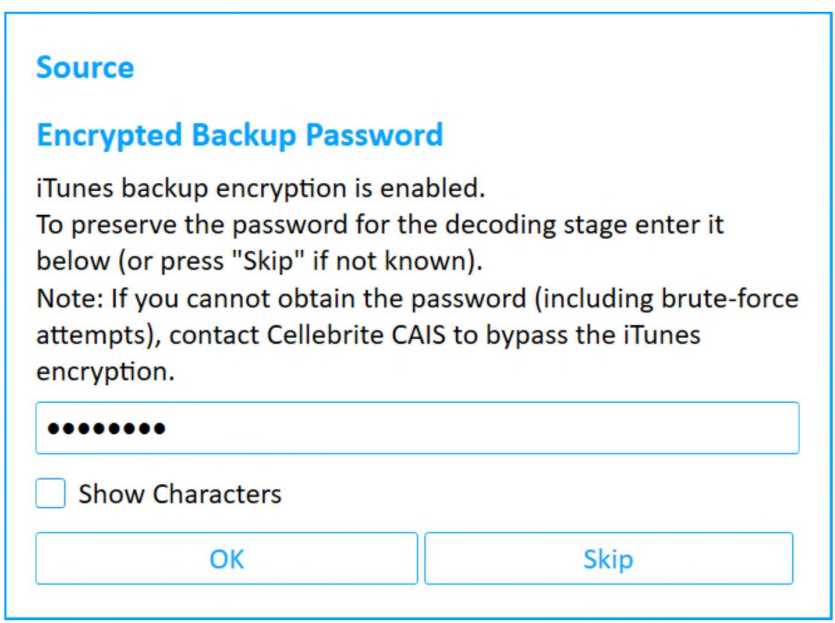
There is an option to encrypt the iOS file. This additional layer of security allows iOS to include more sensitive information not found on a standard iCloud or iTunes backup file, including login details for apps and email accounts and other services that may be in use. You can extract an iOS keychain (user credentials) using this extraction method. At the end of the extraction, the encryption will automatically be reset. You can view the user credentials under the Passwords tree item in Physical Analyzer.

If the extraction was stopped and the device remains encrypted, see Disable iTunes encryption password (on page 126).

EXTRACTION IN PROGRESS Apple iPhone 4 (A1349) using Cable A with black tip T-110 Please wait, this can take some time... /Facebook.app/Facebook



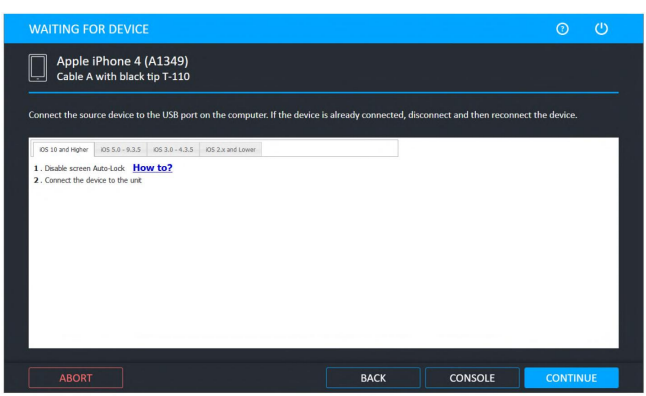
2.2.1. Encrypted iTunes backup During Advanced Logical Extraction, if |Tunes backup encryption is already enabled, then the following window appears: Source Encrypted Backup Password iTunes backup encryption is enabled. To preserve the password for the decoding stage enter it below (or press "Skip" if not known). Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite CAIS to bypass the iTunes encryption. ecceetee '_ | Show Characters If you know the iTunes backup password: 1. Enter the password so that it will not be required during the decoding stage [in Physical Analyzer). 2. Click OK and follow the on-screen instructions to complete the extraction. If you do not know the iTunes backup password: » Click Skip and follow the on-screen instructions to complete the extraction. The password will be required during the decoding stage [in Physical Analyzer). If you have exhausted all options to obtain the password [including the bruteforce option}, Cellebrite Services can provide a full file system extraction that will bypass the iTunes encryption. Chapter 2: 20 Oe


Source
Encrypted Backup Password
iTunes backup encryption is enabled.
To preserve the password for the decoding stage enter it below (or press "Skip" if not known).
Note: If you cannot obtain the password (including brute-force attempts), contact Cellebrite CAIS to bypass the iTunes encryption.
Show Characters
OK
Skip

The password will be required during the decoding stage (in Physical Analyzer).

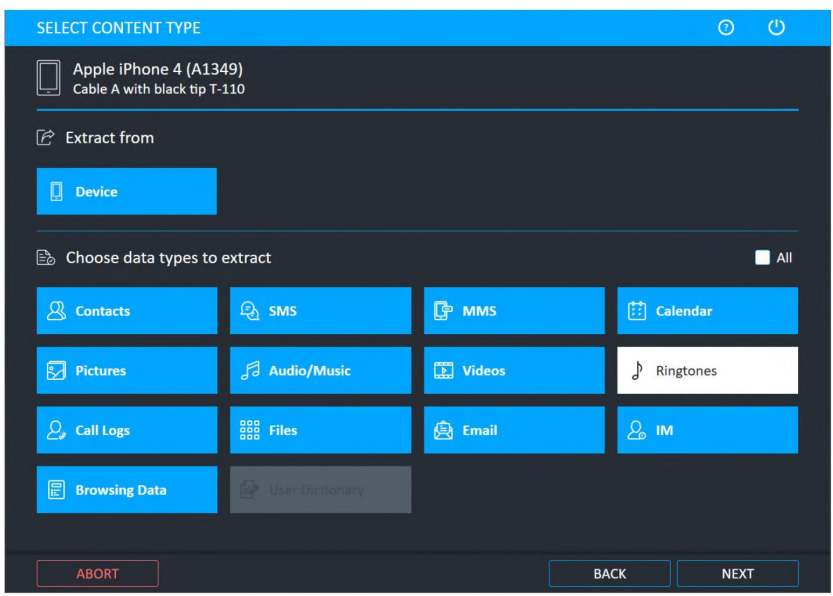
If you have exhausted all options to obtain the password (including the bruteforce option), Cellebrite Services can provide a full file system extraction that will bypass the iTunes encryption.

2.3. Logical (Partial) This is a quick extraction method that supports the largest number of devices. You can extract Call logs, Phone books, SMSs, Calendar events, Multimedia files, and file data. The available types of data may vary depending on the source device's make and model. In most cases, a logical extraction is not possible for locked devices. To perform Logical (Partial) extraction: 1. Click Mobile device and identify the device. 2. Click Logical (Partial) and then select where you want to save the extraction. For information on using optional timeframe and party filters, refer to the Overview Guide. The Select Extraction Location window appears. 3. Use the current location or click the folder icon to change the target path and select a different location and then click Next. The Waiting for Device window appears. WAITING FOR DEVICE Apple iPhone 4 (A1349) Cable A with black tip T-110 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. 10S 10 and Higher | (0S5.0-9.3.5 1053.0-4.3.5 10S 2.x and Lower 1. Disable screen Auto-Lock How to? 2. Connect the device to the unit CONSOLE CONTINUE The Console button Is only supported on Android devices. 4. Select the correct cable and tip for the mobile device, and change the device settings according to the instructions. 5. Connect the source device to a USB port. If the device is already connected, disconnect and then reconnect the device. 6. Click Continue. The following window appears. 21

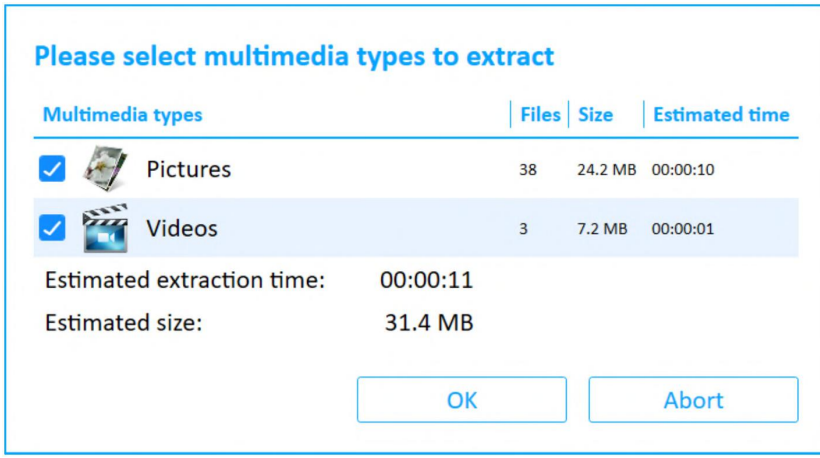

WAITING FOR DEVICE
Apple iPhone 4 (A1349)
Cable A with black tip T-110
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
iOS 10 and Higher
iOS 5.0 - 9.3.5
iOS 3.0 - 4.3.5
iOS 2.x and Lower
1 . Disable screen Auto-Lock How to?
2 . Connect the device to the unit
ABORT
BACK
CONSOLE
CONTINUE

The Console button is only supported on Android devices.

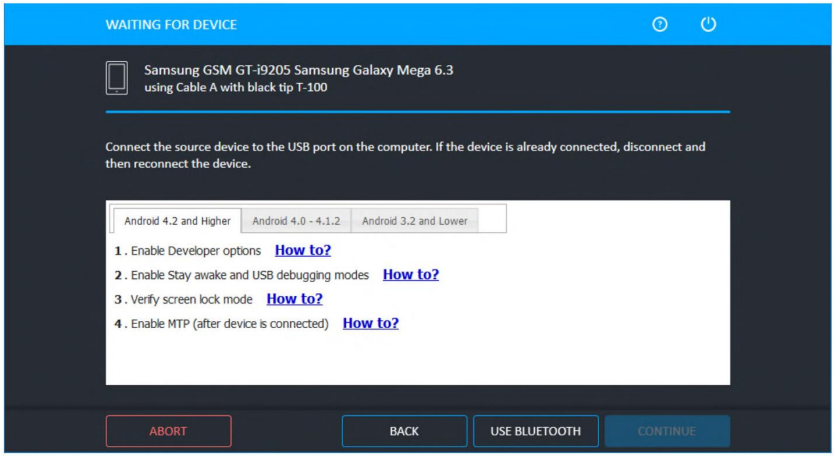
SELECT CONTENT TYPE Apple iPhone 4 (A1349) Cable A with black tip T-110 (f Extract from Device Choose data types to extract & Contacts Q, sms (mms [2] Calendar eA Pictures fa Audio/ Music fe] Videos {oy Call Logs 388 Files & Email 30) IM Browsing Data 7. Different data types can be extracted. Select which data types you want to extract. In the example above Ringtones are excluded and will not be extracted. When the Files button is selected, UFED performs an iTunes backup to extract user data. 8. Click Next. The following window appears. Source Instructions Please unlock the device and choose ‘Trust’ when the trust message displays. Note: Devices with iOS 11 may also require the device password. If the password is requested enter it to proceed with the extraction. 9. Unlock the device and select Trust on the source device. Chapter 2: a

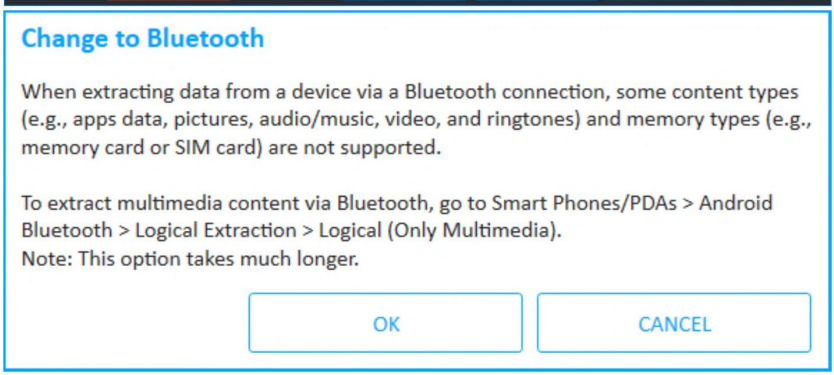


Please select multimedia types to extract Multimedia types | Files | Size | Estimated time tf Pictures 38 24.2MB_ 00:00:10 < < ac] Videos 7.2MB 00:00:01 Estimated extraction time: 00:00:11 Estimated size: 31.4 MB 10. Select the multimedia types required and then click OK. 23

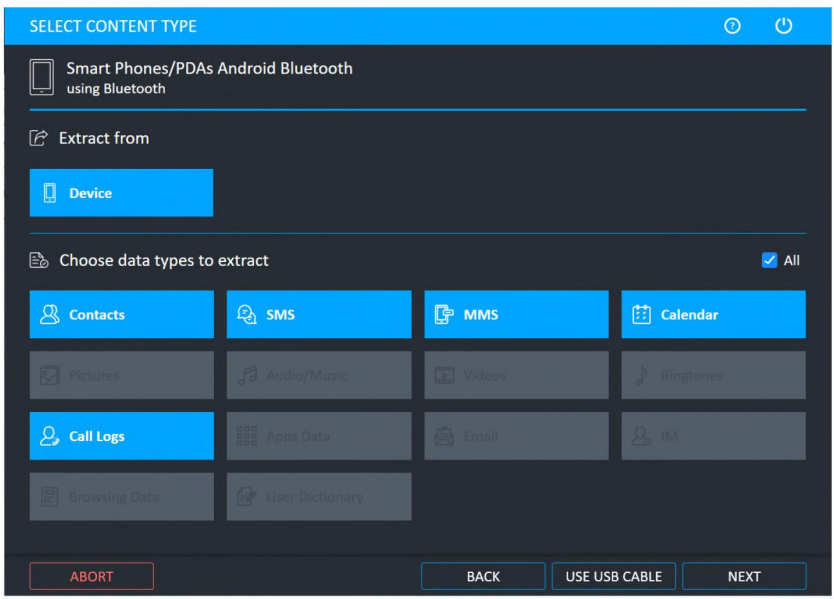


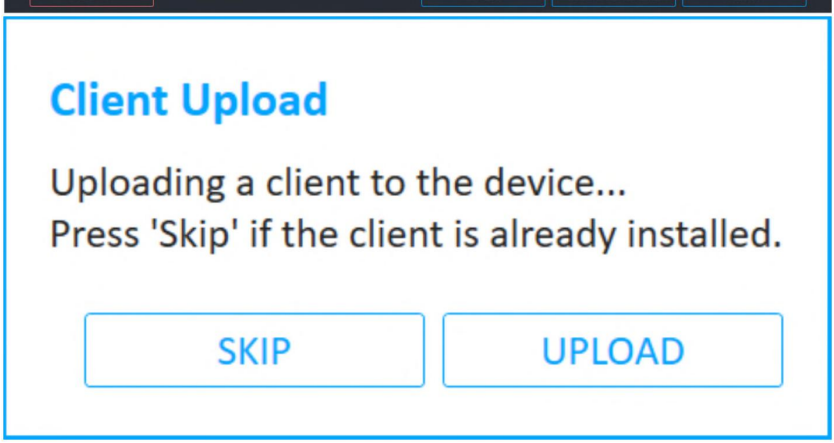
2.4. Logical extraction via Bluetooth This extraction option can be used to perform logical extraction via Bluetooth from any Android device. To use this extraction method, you need to load a client onto the source device over the Bluetooth connection. When extracting data from a device via a Bluetooth connection, some content types [e.g., apps data, pictures, audio/music, video, and ringtones) and memory types [e.g., memory card or SIM card) are not supported. To extract multimedia content via Bluetooth, go to Smart Phones/PDAs > Android Bluetooth > Logical Extraction > Logical (Only Multimedia). Note that this option takes much longer. Previously, the logical extraction via Bluetooth option was only available via the generic profile. To perform a logical extraction via Bluetooth: 1. Click Mobile device, identify the device and then click Logical. 2. Select the extraction location. The following window appears. WAITING FOR DEVICE (1 Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 L using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. Android 4.2 and Higher Android 4.0 - 4.1.2 Android 3.2 and Lower 1. Enable Developer options How to? 2. Enable Stay awake and USB debugging modes How to? 3. Verify screen lock mode How to? 4. Enable MTP (after device is connected) How to? USE BLUETOOTH 3. Click Use Bluetooth. The following window appears. Change to Bluetooth When extracting data from a device via a Bluetooth connection, some content types (e.g., apps data, pictures, audio/music, video, and ringtones) and memory types (e.g., memory card or SIM card) are not supported. To extract multimedia content via Bluetooth, go to Smart Phones/PDAs > Android Bluetooth > Logical Extraction > Logical (Only Multimedia). Note: This option takes much longer. OK CANCEL Chapter 2: 24


WAITING FOR DEVICE
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
Android 4.2 and Higher
Android 4.0 - 4.1.2
Android 3.2 and Lower
1 . Enable Developer options How to?
2 . Enable Stay awake and USB debugging modes How to?
3 . Verify screen lock mode How to?
4 . Enable MTP (after device is connected) How to?
ABORT
BACK
USE BLUETOOTH
CONTINUE

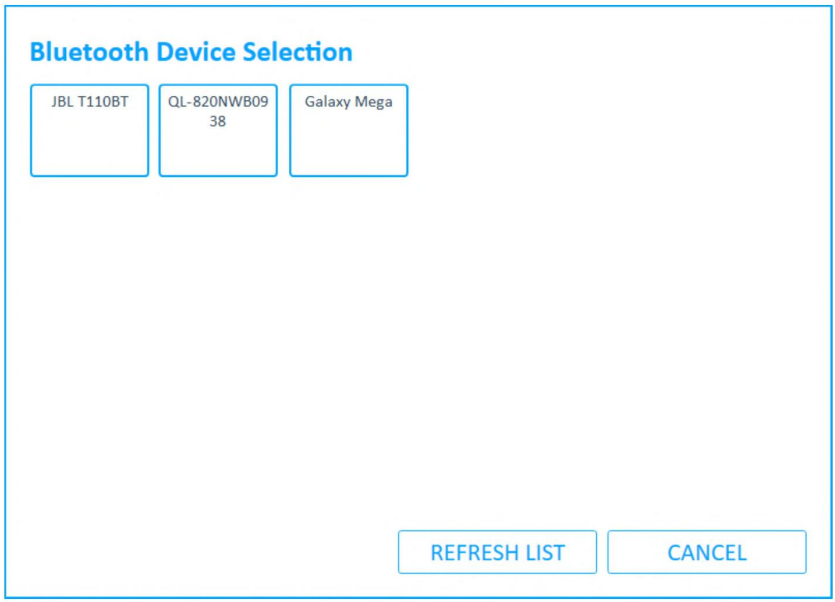

Change to Bluetooth
When extracting data from a device via a Bluetooth connection, some content types (e.g., apps data, pictures, audio/music, video, and ringtones) and memory types (e.g., memory card or SIM card) are not supported.
To extract multimedia content via Bluetooth, go to Smart Phones/PDAs > Android Bluetooth > Logical Extraction > Logical (Only Multimedia).
Note: This option takes much longer.
OK
CANCEL

4. Click OK. The following window appears. SELECT CONTENT TYPE LJ Smart Phones/PDAs Android Bluetooth using Bluetooth (@ Extract from (a Device > Choose data types to extract R Contacts Q SMS Calendar 2 Call Logs USE USB CABLE 5. Select the required content types and then click Next. Client Upload Uploading a client to the device... Press 'Skip' if the client is already installed. SKIP UPLOAD 25

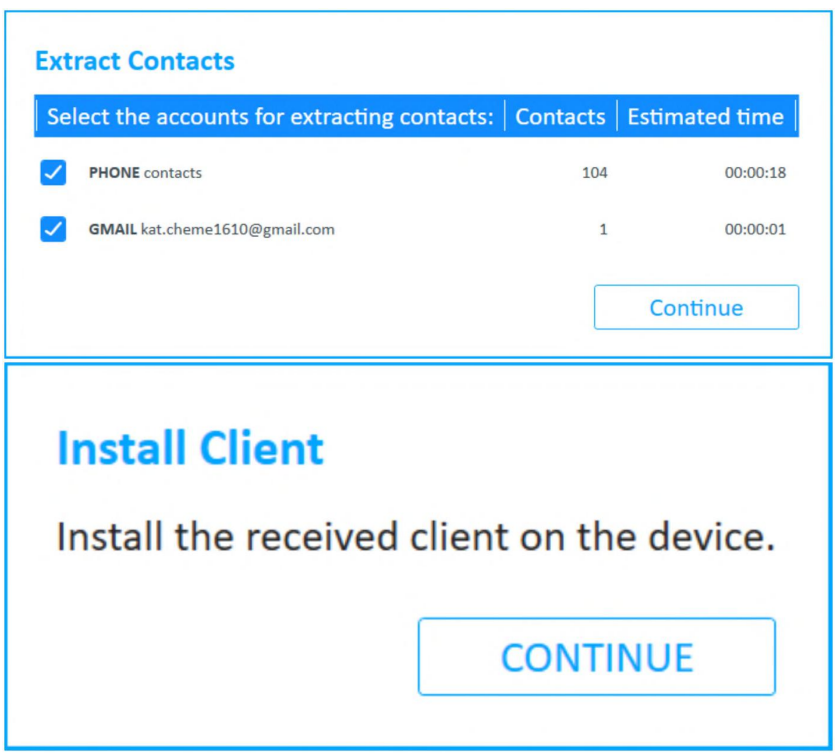




6. Click Upload to upload the client to the device or click Skip if you have already uploaded the client to the device. The following window appears. Connect the device Activate Bluetooth on the SOURCE phone and make it visible to other devices Android Bluetooth: Before connecting the phone, set phone's connection settings as follows: On an Android 4.0 and above, Select the checkbox: "Unknown sources" located under Menu > Settings > Security. On an Android 4.0 and under, Select the checkbox: "Unknown sources" located under Menu > Settings > Applications. Please turn on your Bluetooth connectivity. Make sure your Bluetooth is set to discoverable ON. This phone needs a client in order to communicate with the application. The application has to upload the client to the phone prior to using it. CONTINUE 7. Activate Bluetooth on the source device and make it visible to other devices. Follow the on-screen instructions to set the devices connections, then click Continue. The following window appears. Bluetooth Device Selection JBL T110BT QL-820NWBO09 Galaxy Mega 38 REFRESH LIST | | CANCEL 8. Click the required device. The following window appears. Warning Press Accept on the device when the file transfer request is displayed 9. Press Accept on the device when the file transfer request is displayed (this is skipped if the client is already installed). The following window appears. Chapter 2: 26 SSS eee

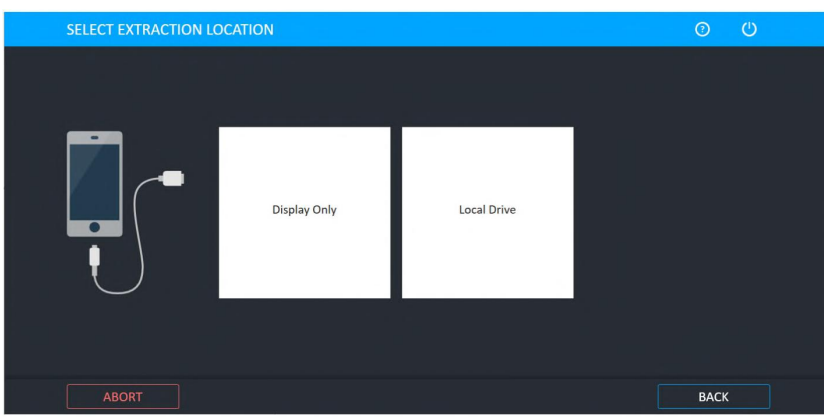

Bluetooth Device Selection
JBL T110BT
QL-820NWB0938
Galaxy Mega
REFRESH LIST
CANCEL

10. 11. Z. Install Client Install the received client on the device. CONTINUE Follow the instructions to install the client on the source device, then click Continue. Start Client Start client application on the SOURCE device CONTINUE Open [or start] the client on the source device and confirm the Bluetooth permission request on the device. Click Continue. The following window appears. Extract Contacts | Select the accounts for extracting contacts: | Contacts | Estimated time PHONE contacts GMAIL kat.cheme1610@gmail.com Continue . Click Continue. During the extraction process, the progress bar for the Source and then the Target Is active. When the extraction is complete and if required, the Source Instructions screen appears (this depends on the device model). 27

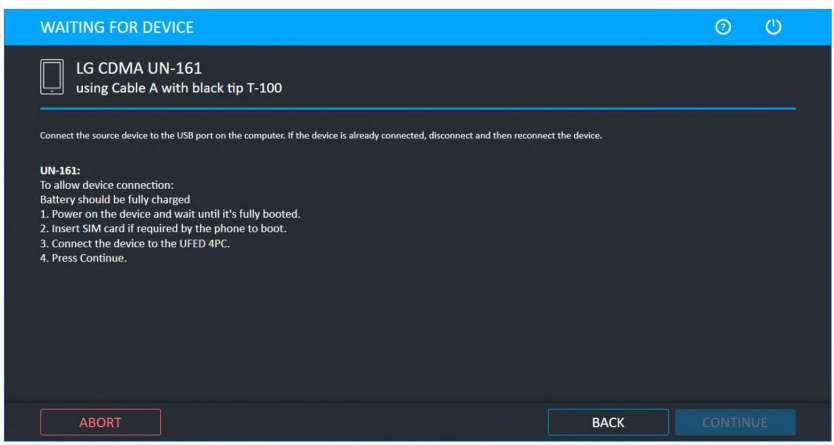


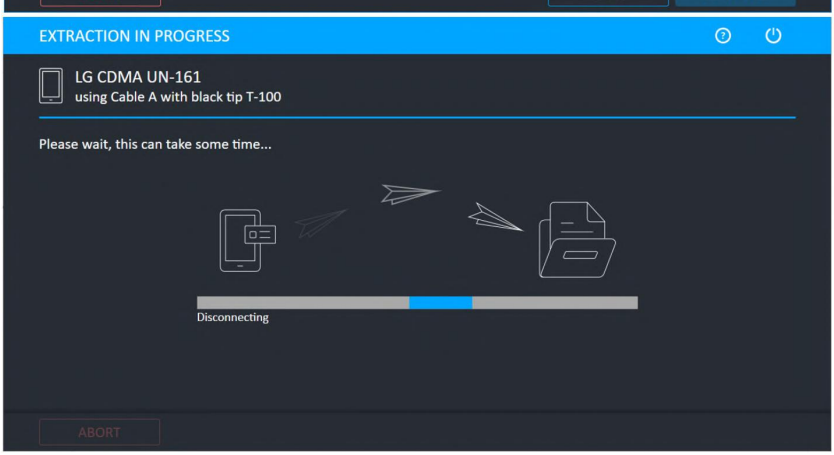
Source Instructions Android Bluetooth: Please don't forget to remove the client! also: Please restore the connection settings: On an Android 4.0 and above, Uncheck the checkbox: "Unknown sources" located under Menu -> Settings > Security. On an Android 4.0 and under, Uncheck the checkbox: "Unknown sources" located under Menu > Settings > Applications. CONTINUE
Chapter 2: 28 SasaanannnnnnnnnnnnnnnnnUnnU nnn cn
Secitnnnencanntittnnttttttttttnniinnttttntttntnttttnttttttttttntttttttttntntttttnttttt
ttt tt

3. Password extraction It is common to encounter a device that is password protected. Passcodes include a 4-digit PIN, a complex alpha/numeric passcode, or a pattern lock. UFED can identify and bypass some passcodes depending on the make and model of the device. To find out if the passcode can be Identified or bypassed, refer to the UFED Supported Devices file. Password extraction includes the following: Extracting the user lock (below) Disabling or re-enabling the user lock [on page 33) Removing the screen lock [on page 35) 3.1. Extracting the user lock Extract the password, or user code/pin, locking the device. The extracted password can be displayed on the screen or written to a USB flash drive or PC for archiving. The ability to extract passwords depends on the device's make and model, the type of passwords enabled on the device, and the password’s length. To extract a user lock on a mobile device: 1. Click Mobile device and identify the device, then click Extract User Lock. The Select Extraction Location screen appears. SELECT EXTRACTION LOCATION aly _ The Waiting for Device screen appears. 29

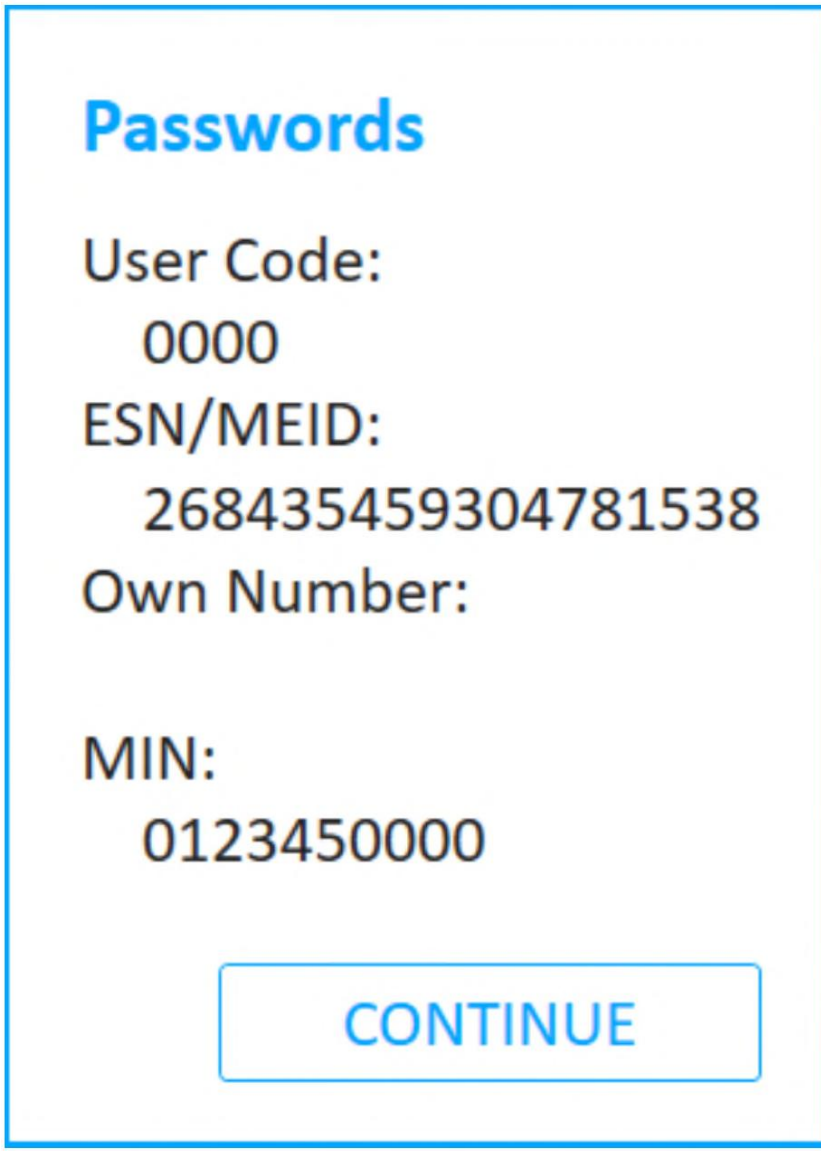


WAITING FOR DEVICE UJ LG CDMA UN-161 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. UN-161: To allow device connection: Battery should be fully charged 1. Power on the device and wait until it's fully booted. 2. Insert SIM card if required by the phone to boot. 3. Connect the device to the UFED 4PC. 4. Press Continue. Connect the source device to the USB port. Click Continue. The Extraction in Progress screen appears. EXTRACTION IN PROGRESS LG CDMA UN-161 using Cable A with black tip T-100 Please wait, this can take some time... Disconnecting At the end of the extraction process, the extracted passwords are displayed in the Passwords screen. Chapter 3: 30


WAITING FOR DEVICE
LG CDMA UN-161
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
UN-161:
To allow device connection:
Battery should be fully charged
1. Power on the device and wait until it's fully booted.
2. Insert SIM card if required by the phone to boot.
3. Connect the device to the UFED 4PC.
4. Press Continue.
ABORT
BACK
CONTINUE



4. Passwords User Code: 0000 ESN/MEID: 268435459304781538 Own Number: MIN: 0123450000 CONTINUE Click Continue to display a summary of the passwords extraction process. ol

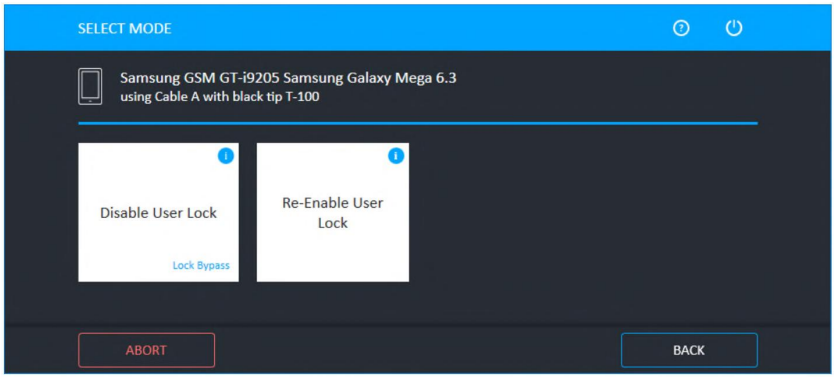


The following screen appears. 5. Click Additional Extractions to add additional extraction types for the same device, or click Finish to end the process and return to the Home screen. 3.1.1. The extracted passwords folder At the end of the passwords extraction process, the extracted passwords are saved to a text file named Passwords.txt at the location you selected during the data extraction process. The text file is located inside a folder named “Password” with the name of the selected device name and the extraction date. For example, “Passwords Iden i? 2011_06_11 (001)"

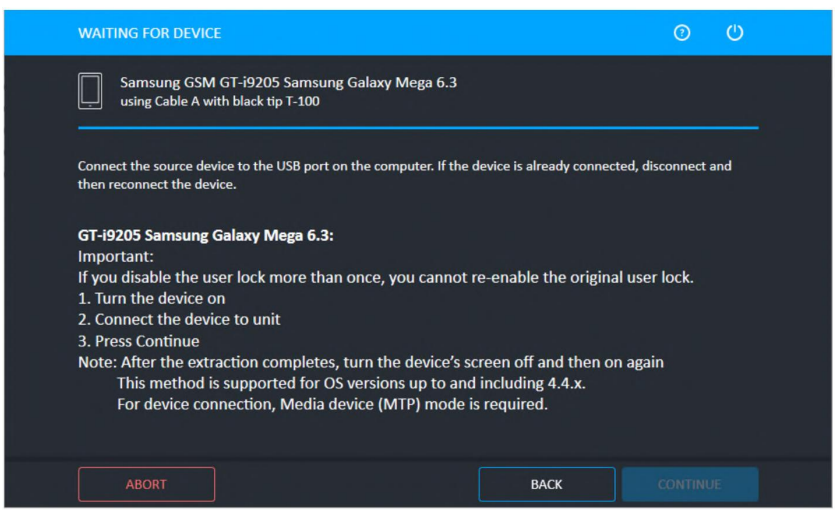
3.2. Disabling or re-enabling the user lock You can disable and re-enable the user lock ona device, as follows: » Disable the user lock: Disable the user lock {or password], which means that the device will no longer be locked. Each device model has a slightly different process, depending on the device lock combination and how the model connects to UFED. When more than one method is available for the device, it is recommended to try both methods If one method is not successful. If you disable the user lock more than once, you cannot re-enable the original user lock. For a complete list of supported devices, refer to UFED Phone Detective or the UFED Supported Devices document in MyCellebrite. >» Re-enable the user lock: Re-enable the user lock on a device, after it was disabled by UFED. This enables you to return a device to Its original state. To re-enable the original user lock on the device, use the Re-Enable User Lock method and do not create a new user lock manually. If you create a new user lock, you cannot re-enable the original user lock. UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and 10S devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/ To disable (or re-enable) the user lock on the device: 1. Click Mobile device and identify the device, then click Disable/Re-enable User Lock. The following window appears. SELECT MODE [Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Re-Enable User Lock Disable User Lock Lock Bypass 2. Click Disable User Lock to remove the user lock from the device, or click Re-Enable User Lock to re-enable the user lock on the device. The Waiting for Device screen appears. oie

To re-enable the original user lock on the device, use the Re-Enable User Lock method and do not create a new user lock manually. If you create a new user lock, you cannot re-enable the original user lock.

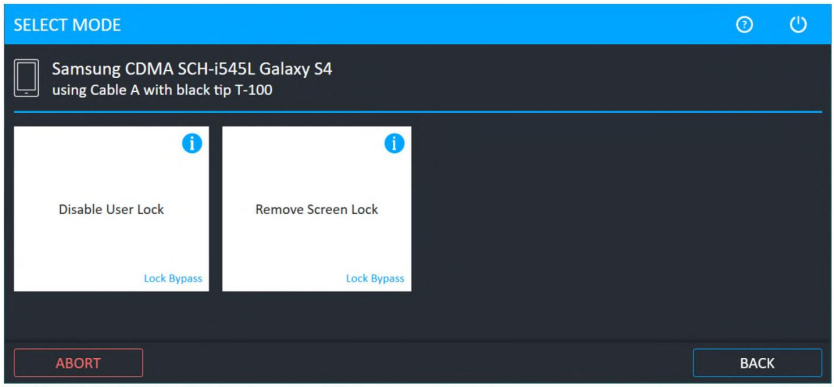
UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/

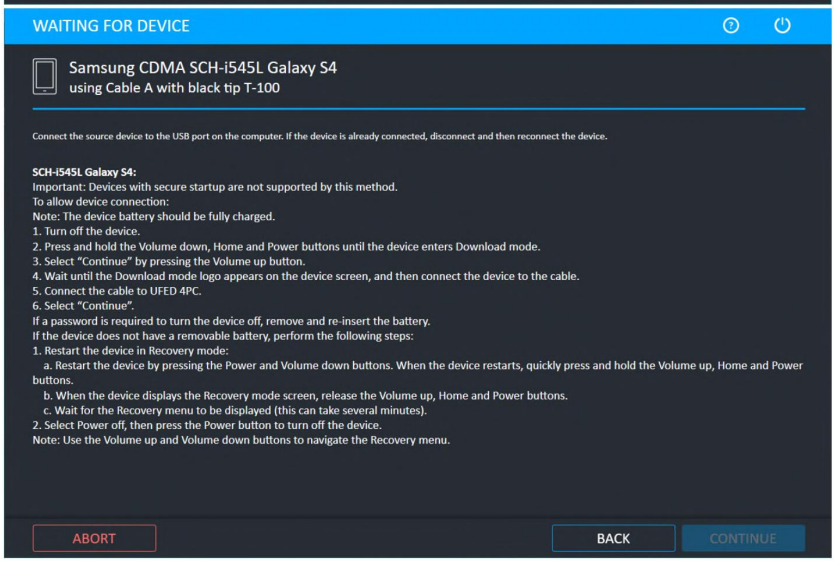

SELECT MODE
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Disable User Lock
Lock Bypass
Re-Enable User Lock
ABORT
BACK

WAITING FOR DEVICE Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. GT-i9205 Samsung Galaxy Mega 6.3: Important: If you disable the user lock more than once, you cannot re-enable the original user lock. 1. Turn the device on 2. Connect the device to unit 3. Press Continue Note: After the extraction completes, turn the device's screen off and then on again This method is supported for OS versions up to and including 4.4.x. For device connection, Media device (MTP) mode is required. 3. Follow the instructions for the device and then click Continue. If the device does not unlock, click Abort, and repeat the procedure. Make sure you are using the correct USB cable. The Extraction completed successfully screen appears. 4. Click Finish. Chapter 3: 34


WAITING FOR DEVICE
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
GT-i9205 Samsung Galaxy Mega 6.3:
Important:
If you disable the user lock more than once, you cannot re-enable the original user lock.
1. Turn the device on
2. Connect the device to unit
3. Press Continue
Note: After the extraction completes, turn the device's screen off and then on again
This method is supported for OS versions up to and including 4.4.x.
For device connection, Media device (MTP) mode is required.
ABORT
BACK
CONTINUE

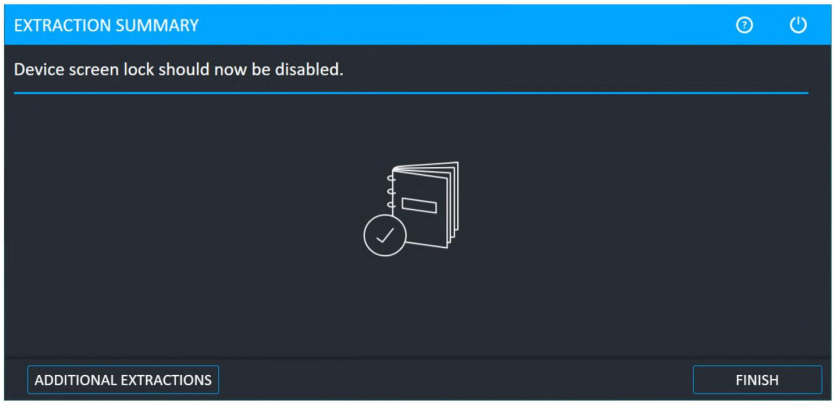
3.3. Removing the screen lock The Remove screen lock method disables the user lock from a wide range of Samsung Android devices for example Galaxy S7, S7 Edge, J7, J5, A7, and AS. This method works on both Qualcomm and Exynos-based devices. UFED cannot re-enable the screen lock after running the process. To remove the screen lock from a device: 1. Click Mobile device and identify the device, then click Disable/Re-enable User Lock. The following window appears. SELECT MODE LJ Samsung CDMA SCH-i545L Galaxy $4 using Cable A with black tip T-100 Disable User Lock Remove Screen Lock Lock Bypass Lock Bypass 2. Click Remove Screen Lock to remove the screen lock from the device. The Waiting for Device window appears. WAITING FOR DEVICE Samsung CDMA SCH-i545L Galaxy $4 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. SCH-i545L Galaxy S4: Important: Devices with secure startup are not supported by this method. To allow device connection: Note: The device battery should be fully charged. 1. Turn off the device. 2. Press and hold the Volume down, Home and Power buttons until the device enters Download mode. 3. Select “Continue” by pressing the Volume up button. 4. Wait until the Download mode logo appears on the device screen, and then connect the device to the cable. 5. Connect the cable to UFED 4PC. 6. Select “Continue”. If a password is required to turn the device off, remove and re-insert the battery. If the device does not have a removable battery, perform the following steps: 1. Restart the device in Recovery mode: a. Restart the device by pressing the Power and Volume down buttons. When the device restarts, quickly press and hold the Volume up, Home and Power buttons. b. When the device displays the Recovery mode screen, release the Volume up, Home and Power buttons. c. Wait for the Recovery menu to be displayed (this can take several minutes). 2. Select Power off, then press the Power button to turn off the device. Note: Use the Volume up and Volume down buttons to navigate the Recovery menu. Sis


SELECT MODE
Samsung CDMA SCH-i545L Galaxy S4
using Cable A with black tip T-100
Disable User Lock
Lock Bypass
Remove Screen Lock
Lock Bypass
ABORT
BACK

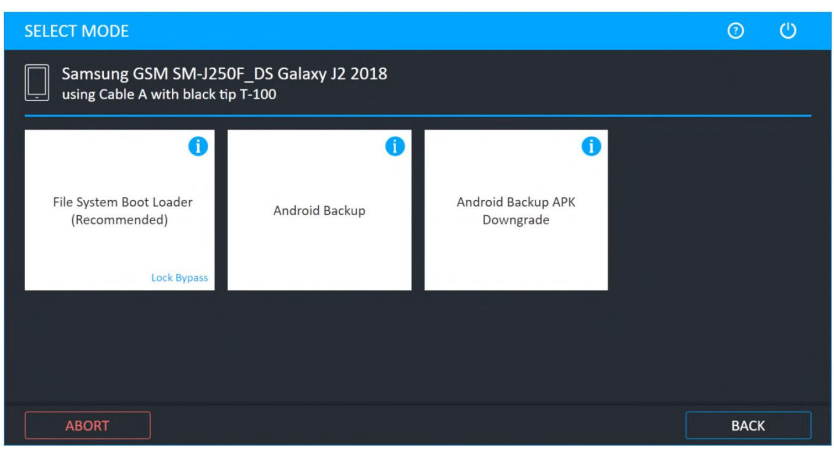

WAITING FOR DEVICE
Samsung CDMA SCH-i545L Galaxy S4
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
SCH-i545L Galaxy S4:
Important: Devices with secure startup are not supported by this method.
To allow device connection:
Note: The device battery should be fully charged.
1. Turn off the device.
2. Press and hold the Volume down, Home and Power buttons until the device enters Download mode.
3. Select "Continue" by pressing the Volume up button.
4. Wait until the Download mode logo appears on the device screen, and then connect the device to the cable.
5. Connect the cable to UFED 4PC.
6. Select "Continue".
If a password is required to turn the device off, remove and re-insert the battery.
If the device does not have a removable battery, perform the following steps:
1. Restart the device in Recovery mode:
a. Restart the device by pressing the Power and Volume down buttons. When the device restarts, quickly press and hold the Volume up, Home and Power buttons.
b. When the device displays the Recovery mode screen, release the Volume up, Home and Power buttons.
c. Wait for the Recovery menu to be displayed (this can take several minutes).
2. Select Power off, then press the Power button to turn off the device.
Note: Use the Volume up and Volume down buttons to navigate the Recovery menu.
ABORT
BACK
CONTINUE

3. Follow the instructions to place the device in Download mode, then click Continue. The following window appears. Attention UFED will now try to flash another image to the device. Press and hold the Volume down, Power and Home (or Bixby) buttons, until the device displays the Warning screen. Then press Volume up and select "Continue" in UFED. CONTINUE 4. UFED will now try to flash another image to the device. Follow the on-screen instructions until the device the device displays the Warning screen and Download mode again. Then click Continue in UFED. The following window appears. Attention The process has ended. The device will now restart. Wait about one minute and then restart the device again when instructed. CONTINUE 5. Click Continue, then wait about one minute and restart the device again when instructed. The following window appears. Attention Restart the device for the changes to take effect. CONTINUE 6. Restart the device for the changes to take effect and then click Continue. The following window appears. Device Instructions SCH-i545L Galaxy S4: The process completed and the device screen lock should now be disabled. Due to the nature of the process, UFED 4PC can’t determine if it was successful. If for some reason it didn’t work try a different extraction method. Chapter 3: 36

ie 8. The process completed successfully, but it may not work on all devices. Ifthe process did not work, try a different method. Click OK. The following window appears. EXTRACTION SUMMARY Device screen lock should now be disabled. &] ADDITIONAL EXTRACTIONS FINISH Click Finish. oi

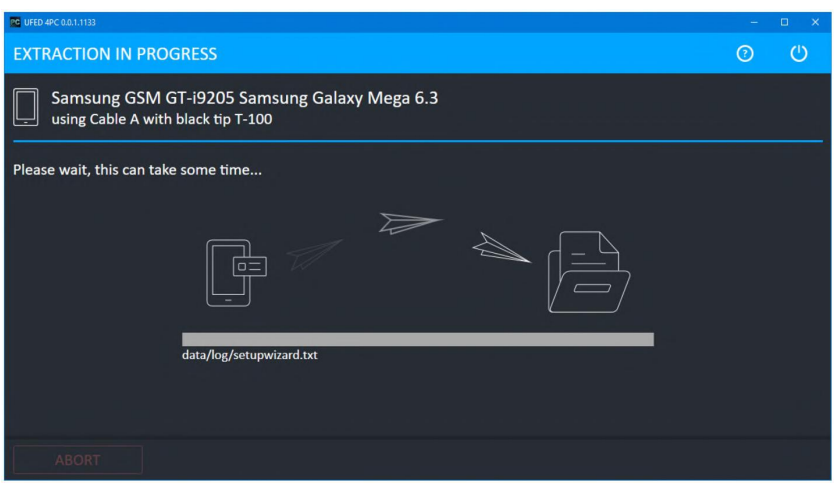


4. File system extraction The File system extraction enables you to perform a full system extraction from a device. File system extractions include the following: Performing a file system extraction [below] Android backup [on page 41) Android backup APK downgrade (on page 45) Selective file system extraction [on page 56) UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/ Lock Bypass Is displayed if the file system extraction method can bypass the user lock of the device. 4.1. Performing a file system extraction 1. Click Mobile device and identify the device, then click File System. The Select Mode screen appears. SELECT MODE Samsung GSM SM-J250F_DS Galaxy J2 2018 using Cable A with black tip T-100 File System Boot Loader . Android Backup APK Android Back' (Recommended) ee Downgrade Lock Bypass 2. Select ADB [for Android Backup, see Android backup [on page 41)). For information on using optional timeframe and party filters, refer to the Overview Guide. Chapter 4: 38

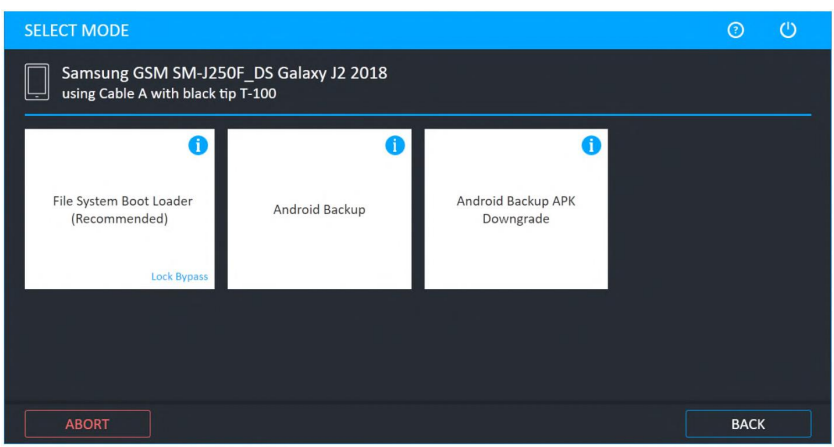


The Select Extraction Location screen appears. 3. Select a location. The following window appears. WAITING FOR DEVICE (| Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. Android 4.2 and Higher | 4,1,2 and Lower ® Tutorial Video 1. Enable Developer options How to? 2. Enable Stay awake and USB debugging modes How to? 3. Verify screen lock mode How to? 4. Connect the device to the unit. BACK the screen. 5. Change the device settings according to the instructions Select the correct cable and tip for the mobile device based on the information written in 37

6. Click Continue. The Extraction in Progress screen appears. UFED 4PC 0.0.1.1133 EXTRACTION IN PROGRESS LJ Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Please wait, this can take some time... data/ log/setupwizard.txt During the extraction process, the progress bar for the Source and then the Target is active. For QCP and Samsung MTK devices, an estimation of the time the extraction will take is displayed. When extraction is complete, the File System Extraction Summary screen appears. 4.1.1. The file system extraction folder At the end of the file system extraction process, the extracted data Is saved in the location you selected previously [see Performing a file system extraction (on page 38)). The extracted data folder is named “FileSystemDump" with the selected device model and name and the extraction operation date. For example, "FileSystemDump Nokia GSM Nokia 2626 2014_03_12 (001)" The extracted data folder contains: » Zipped archive of the device file system containing files and folders in the same structure they were extracted. » UFD file containing the system extraction information, used by the Physical Analyzer application. » PM file. The File System extraction can be viewed using Physical Analyzer. Chapter 4: 40 Snr nncennnnTTTTTnnnnnnnnnTtnnntnnntnnnn Senn


UFED 4PC 0.0.1.1133
EXTRACTION IN PROGRESS
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Please wait, this can take some time...
data/log/setupwizard.txt
ABORT

4.2. Android backup The Android Backup feature communicates with a connected Android device and enables you to extract data from the device. The data that is extracted is dependent on the device's specific characteristics. Android backup supports Android devices with version 4.1 and later. Android Backup may provide less data then other methods, therefore, you should use this feature when other file system methods such as ADB are not successful, or when other file system methods are not available for the device (for example, if the android version is not supported). This feature is controlled under Settings > General. To extract data using Android backup: iP Click Mobile device and identify the device, then click File System. SELECT MODE Samsung GSM SM-J250F_DS Galaxy J2 2018 using Cable A with black tip T-100 Android Backup APK Downgrade File System Boot Loader (Recommended) Android Backup Lock Bypass 2. Click Android Backup. 3. Select the extraction location. 4. For information on using optional timeframe and party filters, refer to the Overview Guide. Click Continue. 4]



The Waiting for Device screen appears. Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. GT-i9205 Samsung Galaxy Mega 6.3: Important: Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode. This method is supported for devices running Android version 4.1 and above and with Developer options enabled. To enable the Developer options, go to Menu - Settings > About (information) > tap the "Build number" 7 times until it's enabled. Under Developer options > enable the Android/ USB debugging and Stay awake (if available). Notice: After pressing "Continue" the extraction will start automatically, DO NOT press anything. If the extraction does not start you will be prompted to select "Back up my data" on the device. Note: On some devices the "Back up my data" button may be disabled. To enable it, enter a password and then press the "Back up my data" button. To decode the extraction, this password will also be required in UFED 4PC Physical Analyzer. On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue. BACK | 5. Connect the source device to the USB port. If the device is already connected, disconnect and then reconnect the device. 6. Click Continue. The following window appears. The extraction will start automatically. Ignore any Android system messages on the device and DO NOT press any button. If the extraction does not start you will be prompted to select "Back up my data" on the device to start the process. 7. Click Continue and if required select Backup my data on the device. The extraction begins. Huawei EVA-L19 P9 using USB cable 170 or Original Cable Please wait, this can take some time... Connecting The following screen appears. Chapter 4: 42 Snr nnncnnnnTTTTTTnnnnnnnnTntnnntnnntnnnnnn Senn

Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

GT-i9205 Samsung Galaxy Mega 6.3:
Important:
Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode.
This method is supported for devices running Android version 4.1 and above and with Developer options enabled.
To enable the Developer options, go to Menu → Settings → About (information) → tap the "Build number" 7 times until it's enabled.
Under Developer options → enable the Android/USB debugging and Stay awake (if available).
Notice:
After pressing "Continue" the extraction will start automatically, DO NOT press anything.
If the extraction does not start you will be prompted to select "Back up my data" on the device.
Note:
On some devices the "Back up my data" button may be disabled.
To enable it, enter a password and then press the "Back up my data" button.
To decode the extraction, this password will also be required in UFED 4PC Physical Analyzer.
On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue.

ABORT BACK CONTINUE

Huawei EVA-L19 P9
using USB cable 170 or Original Cable

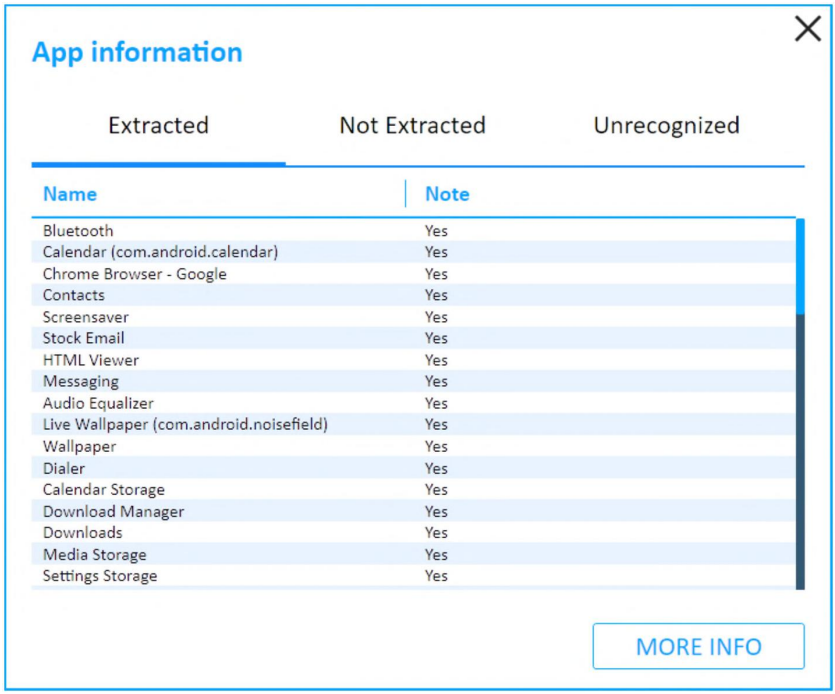
Please wait, this can take some time...

Connecting

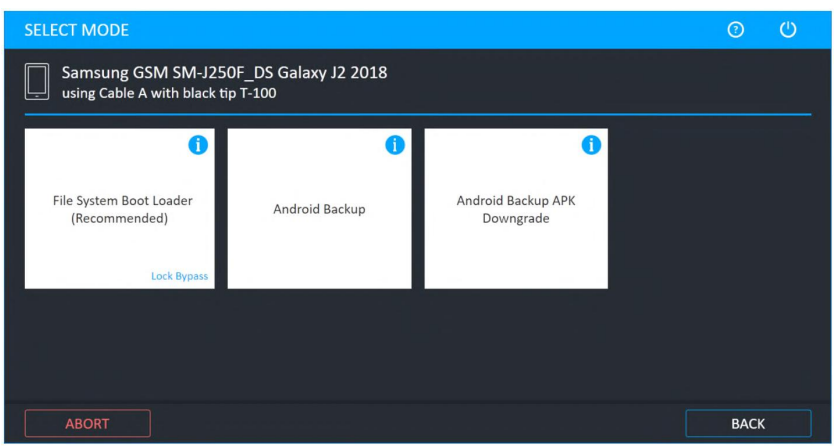
ABORT

Android backup Would you like to try data extraction from a shared location? The system will attempt to extract data from the device’s internal storage and memory card and will take additional time. 8. Click No if you do not want to extract data from a shared location. Click Yes if you want to try extract data from a shared location. With a shared location, Cellebrite UFED/Responder extracts all the applications (native and non-native} that reside on the device, as well as data from the device's internal storage and memory card limages, videos, etc.}, which takes additional time. The following screen appears. Device Instructions GT-i9205 Samsung Galaxy Mega 6.3: Please return the Screen timeout to its original settings: Menu (Apps) > Settings > My Device > Display > Screen timeout. or Menu (Apps) > Settings > Display > Screen timeout. or Menu (Apps) > Settings > Display > Sleep. 9. Follow the instructions and click OK. When the extraction completes the Extraction summary window appears. 43

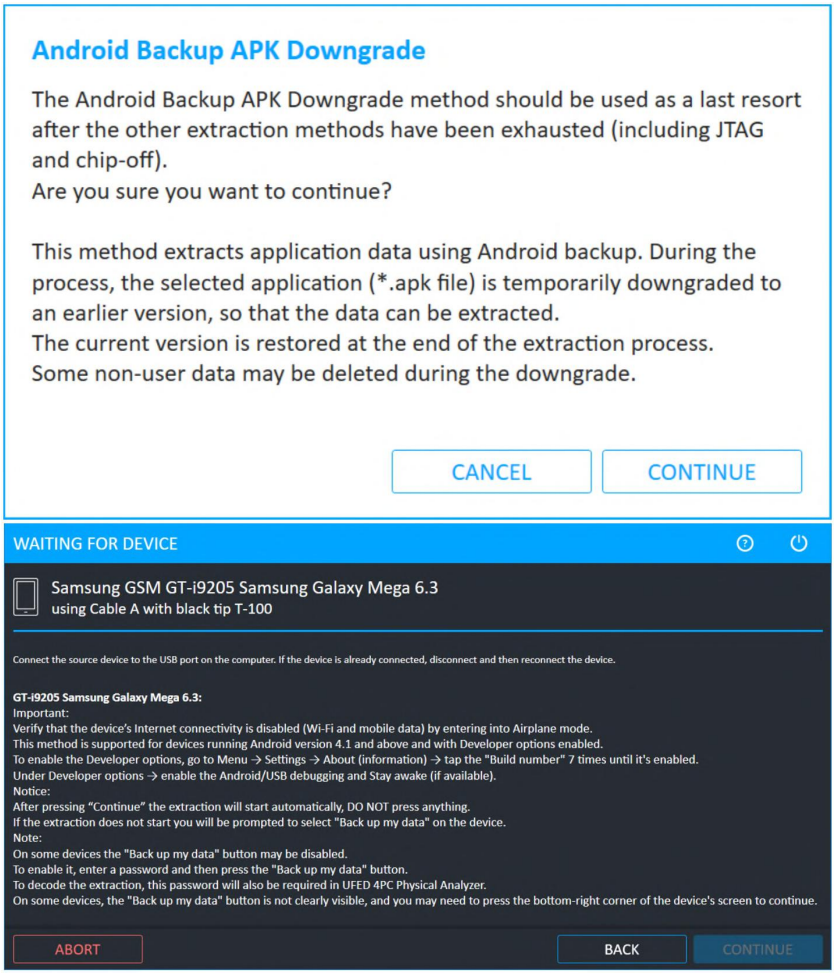
4.2.1. Extracted apps The App information window can be displayed by clicking the Extracted Apps button after the File system Android backup extraction completes. It displays the apps extraction status for the device. Apps that were extracted are listed under “Extracted”. These apps will be decrypted in Physical Analyzer. Apps that could not be extracted are listed under “Not Extracted” and indicates the reason the apps were not extracted. The Notes indicate If another extraction method is applicable. Unrecognized apps and their status are listed under “Unrecognized”. This list contains files that could not be mapped by the system and exist for extraction results verification. To obtain more information about these files it is recommended to do an Internet search for the file names. An example is displayed next. App information Extracted Not Extracted Unrecognized Name | Note Bluetooth Yes Calendar (com.android.calendar) Yes Chrome Browser - Google Yes Contacts Yes Screensaver Yes Stock Email Yes HTML Viewer Yes Messaging Yes Audio Equalizer Yes Live Wallpaper (com.android.noisefield) Wallpaper Yes Dialer Calendar Storage Download Manager Downloads Media Storage Settings Storage MORE INFO Chapter 4: 44 ee


App information
Extracted
Not Extracted
Unrecognized
Name
Note
Bluetooth Yes
Calendar (com.android.calendar) Yes
Chrome Browser - Google Yes
Contacts Yes
Screensaver Yes
Stock Email Yes
HTML Viewer Yes
Messaging Yes
Audio Equalizer Yes
Live Wallpaper (com.android.noisefield) Yes
Wallpaper Yes
Dialer Yes
Calendar Storage Yes
Download Manager Yes
Downloads Yes
Media Storage Yes
Settings Storage Yes
MORE INFO

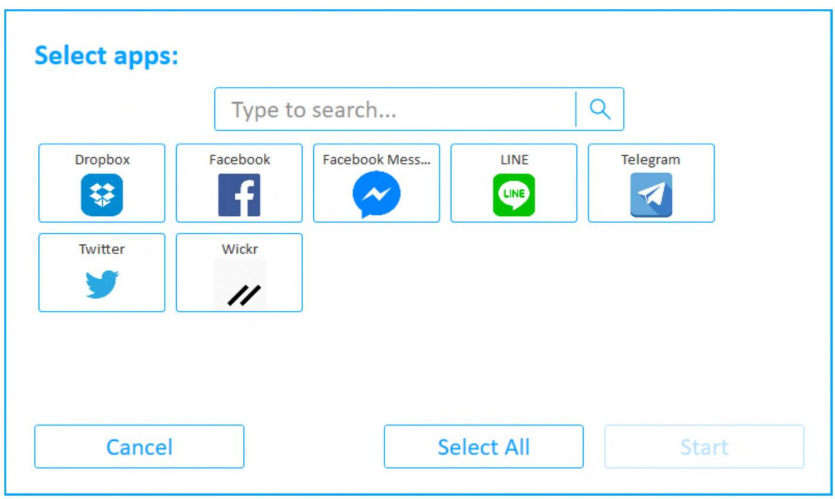
4.3. Android backup APK downgrade This method extracts application data using Android backup. It supports Android devices with version 4.1 and later. During the process, the selected application version [*.apk file) is temporary downgraded to an earlier version, so that the data can be extracted. The current version 1s restored at the end of the extraction process. The potential risk in this method relates to the downgrading and then restoration of the app version. The Android Backup APK Downgrade method should be used only as a last resort after other extraction methods have been exhausted [including JTAG and chip-off). (A) It is recommended to document the process during the extraction. To extract data using Android backup APK downgrade: 1. Click Mobile device and identify the device, then click File System. The following window appears. SELECT MODE Samsung GSM SM-J250F_DS Galaxy J2 2018 using Cable A with black tip T-100 File System Boot Loader (Recommended) Android Backup APK Android Backup Downgrade Lock Bypass 45

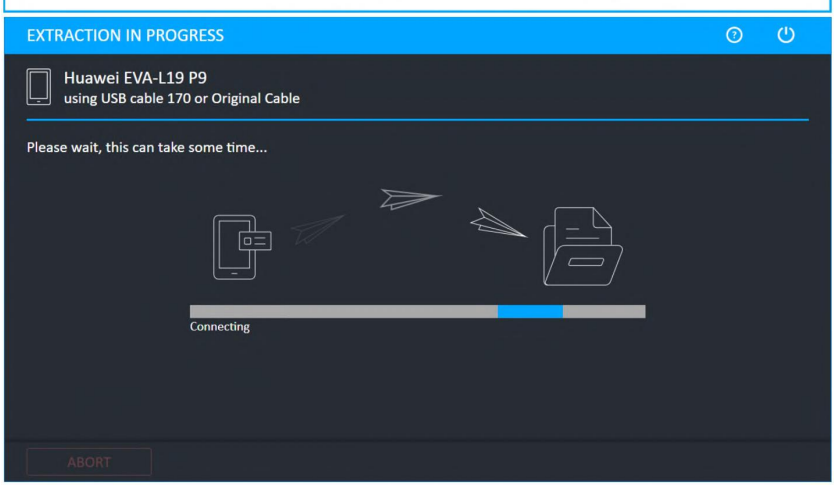


2. Click Android Backup APK Downgrade. The following window appears. Android Backup APK Downgrade The Android Backup APK Downgrade method should be used as a last resort after the other extraction methods have been exhausted (including JTAG and chip-off). Are you sure you want to continue? This method extracts application data using Android backup. During the process, the selected application (*.apk file) is temporarily downgraded to an earlier version, so that the data can be extracted. The current version is restored at the end of the extraction process. Some non-user data may be deleted during the downgrade. CANCEL || _ CONTINUE 3. Click Continue. For information on using optional timeframe and party filters, refer to the Overview Guide. 4. Select the target path. The Waiting for Device screen appears. WAITING FOR DEVICE Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. GT-i9205 Samsung Galaxy Mega 6.3: Important: Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode. This method is supported for devices running Android version 4.1 and above and with Developer options enabled. To enable the Developer options, go to Menu > Settings > About (information) > tap the "Build number" 7 times until it's enabled. Under Developer options > enable the Android/USB debugging and Stay awake (if available). Notice: After pressing "Continue" the extraction will start automatically, DO NOT press anything. If the extraction does not start you will be prompted to select "Back up my data" on the device. Note: On some devices the "Back up my data" button may be disabled. To enable it, enter a password and then press the "Back up my data" button. To decode the extraction, this password will also be required in UFED 4PC Physical Analyzer. On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue. BACK 5. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device. 6. Follow the on-screen instructions for the device and then click Continue. The following screen appears. Chapter 4: 46


Android Backup APK Downgrade
The Android Backup APK Downgrade method should be used as a last resort after the other extraction methods have been exhausted (including JTAG and chip-off).
Are you sure you want to continue?
This method extracts application data using Android backup. During the process, the selected application (*.apk file) is temporarily downgraded to an earlier version, so that the data can be extracted.
The current version is restored at the end of the extraction process.
Some non-user data may be deleted during the downgrade.
CANCEL
CONTINUE
WAITING FOR DEVICE
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
GT-i9205 Samsung Galaxy Mega 6.3:
Important:
Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode.
This method is supported for devices running Android version 4.1 and above and with Developer options enabled.
To enable the Developer options, go to Menu → Settings → About (information) → tap the "Build number" 7 times until it's enabled.
Under Developer options → enable the Android/USB debugging and Stay awake (if available).
Notice:
After pressing "Continue" the extraction will start automatically, DO NOT press anything.
If the extraction does not start you will be prompted to select "Back up my data" on the device.
Note:
On some devices the "Back up my data" button may be disabled.
To enable it, enter a password and then press the "Back up my data" button.
To decode the extraction, this password will also be required in UFED 4PC Physical Analyzer.
On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue.
ABORT
BACK
CONTINUE

You will be notified when you are required to restart the device or to select Backup my data on the device. The following screen appears. The following window appears. Select apps: Type to search... , a4 ＜3 rr Dropbox | | Facebook Facebook Mess... Telegram | Cancel Select All 7. Select the required apps [or click Select All) and then click Start. The following window appears. EXTRACTION IN PROGRESS Huawei EVA-L19 P9 using USB cable 170 or Original Cable Please wait, this can take some time... Connecting 8. Select Backup my data on the device. The following window appears. 47

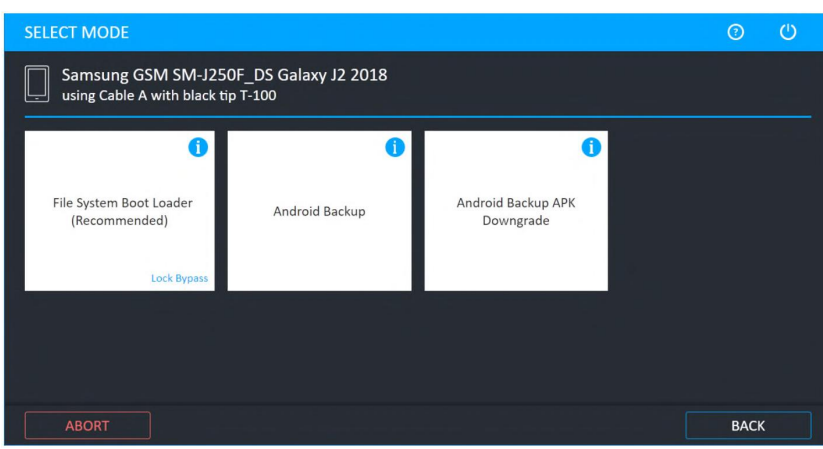


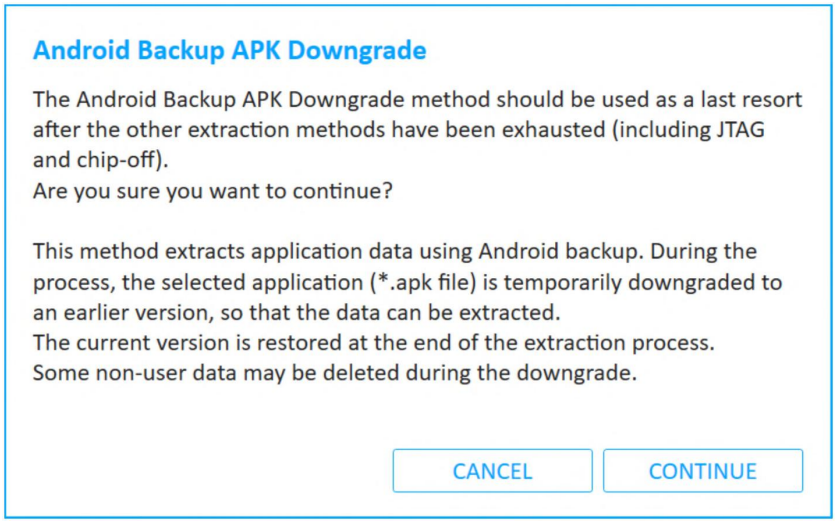


Android backup Would you like to try data extraction from a shared location? The system will attempt to extract data from the device’s internal storage and memory card and will take additional time. fi NO] YES 9. Click No if you do not want to extract data from a shared location. Click Yes if you want to try extract data from a shared location. With a shared location, Cellebrite UFED/ Responder extracts all the applications (native and non-native) that reside on the device, as well as data from the device's internal storage and memory card limages, videos, etc.}, which takes additional time. If some app packages could not be backed up, this screen provides an indication of how many app packages were backed up successfully. 10. Click Continue. The following screen appears. Device Instructions GT-i9205 Samsung Galaxy Mega 6.3: Please return the Screen timeout to its original settings: Menu (Apps) > Settings > My Device > Display > Screen timeout. or Menu (Apps) > Settings > Display > Screen timeout. or Menu (Apps) > Settings > Display > Sleep. Chapter 4: 48

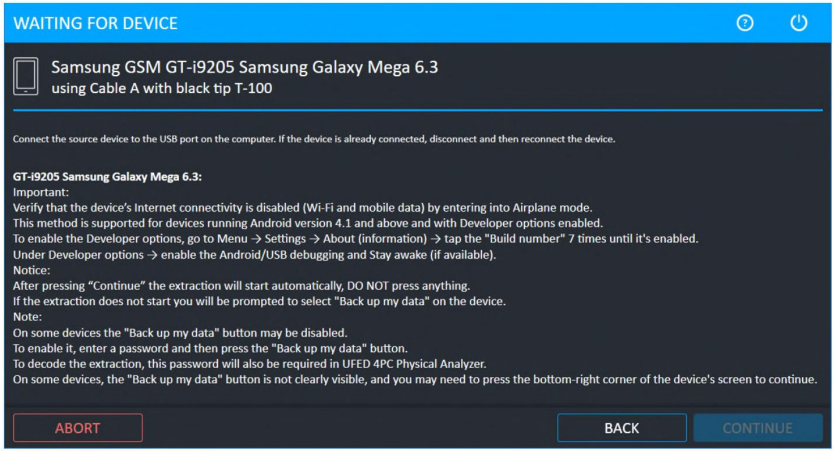
ile Follow the instructions and click OK. The Extraction summary window appears. 49

4.3.1. Android backup APK downgrade - Manual installation Manually intervene during the APK downgrade process to overcome installation issues where the device is not compatible. To extract data using Android backup APK downgrade by manually installing the apps: 1. Click Mobile device and identify the device, then click File System. The following window appears. SELECT MODE ff Samsung GSM SM-J250F_DS Galaxy J2 2018 using Cable A with black tip T-100 Android Backup APK Downgrade File System Boot Loader Android Back (Recommended) PEON BENE, Lock Bypass 2. Click Android Backup APK Downgrade. The following window appears. Android Backup APK Downgrade The Android Backup APK Downgrade method should be used as a last resort after the other extraction methods have been exhausted (including JTAG and chip-off). Are you sure you want to continue? This method extracts application data using Android backup. During the process, the selected application (*.apk file) is temporarily downgraded to an earlier version, so that the data can be extracted. The current version is restored at the end of the extraction process. Some non-user data may be deleted during the downgrade. CANCEL | | CONTINUE 3. Click Continue. For information on using optional timeframe and party filters, refer to the Overview Guide. Chapter 4: 50

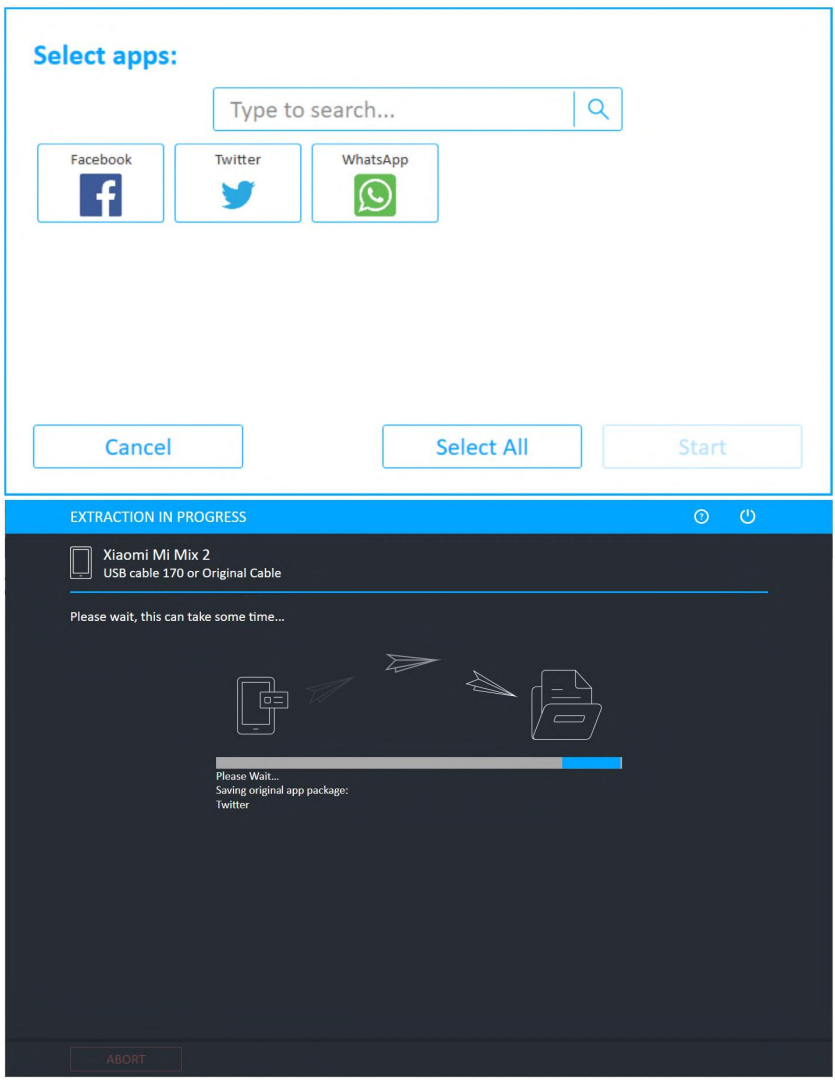



Android Backup APK Downgrade
The Android Backup APK Downgrade method should be used as a last resort after the other extraction methods have been exhausted (including JTAG and chip-off).
Are you sure you want to continue?
This method extracts application data using Android backup. During the process, the selected application (*.apk file) is temporarily downgraded to an earlier version, so that the data can be extracted.
The current version is restored at the end of the extraction process.
Some non-user data may be deleted during the downgrade.
CANCEL
CONTINUE

4. Select the target path. The Waiting for Device screen appears. WAITING FOR DEVICE Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. GT-i9205 Samsung Galaxy Mega 6.3: Important: Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode. This method is supported for devices running Android version 4.1 and above and with Developer options enabled. To enable the Developer options, go to Menu -> Settings > About (information) — tap the "Build number" 7 times until it's enabled. Under Developer options > enable the Android/USB debugging and Stay awake (if available). Notice: After pressing "Continue" the extraction will start automatically, DO NOT press anything. If the extraction does not start you will be prompted to select "Back up my data" on the device. Note: On some devices the "Back up my data" button may be disabled. To enable it, enter a password and then press the "Back up my data" button. To decode the extraction, this password will also be required in UFED 4PC Physical Analyzer. On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue. BACK 5. Connect the source device to the USB port using the specified cable. If the device is already connected, disconnect and then reconnect the device. 6. Follow the on-screen instructions for the device and then click Continue. The following screen appears. Android Backup APK Downgrade Note: For devices having android OS 6.0 and above, user data (credentials) might be lost during the operation. ABORT CONTINUE 7. Click Continue. Attention This device does not support the automatic installation of apps. To proceed with the extraction, you will be prompted to install each app manually. At the end of the process, the original app version will be restored. ABORT | | CONTINUE 8. This notification appears on devices that do not support automatic installation of apps. You will be prompted to install the apps manually. Click Continue. The following window appears. a1


WAITING FOR DEVICE
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
GT-i9205 Samsung Galaxy Mega 6.3:
Important:
Verify that the device's Internet connectivity is disabled (Wi-Fi and mobile data) by entering into Airplane mode.
This method is supported for devices running Android version 4.1 and above and with Developer options enabled.
To enable the Developer options, go to Menu → Settings → About (information) → tap the "Build number" 7 times until it's enabled.
Under Developer options → enable the Android/USB debugging and Stay awake (if available).
Notice:
After pressing "Continue" the extraction will start automatically, DO NOT press anything.
If the extraction does not start you will be prompted to select "Back up my data" on the device.
Note:
On some devices the "Back up my data" button may be disabled.
To enable it, enter a password and then press the "Back up my data" button.
To decode the extraction, this password will also be required in UFED 4PC Physical Analyzer.
On some devices, the "Back up my data" button is not clearly visible, and you may need to press the bottom-right corner of the device's screen to continue.
ABORT
BACK
CONTINUE

Select apps: | Type to search... | Facebook | | Twitter | | WhatsApp Fi v Select All 9. Select the required apps lor click Select All) and then click Start. The following window appears. EXTRACTION IN PROGRESS Oj Xiaomi Mi Mix 2 USB cable 170 or Original Cable Please wait, this can take some time... Ls Please Wait... Saving original app package: Twitter The following window appears. Chapter 4: i Oe



Manual installation required You need to manually install the app (APK file). Go to File manager (also called file explorer, my files etc.) and install the last APK file under All files/ storage called "Install Me.apk". These instructions are repeated twice for each app that requires manual installation (first the app is downgraded then the original app is restored). Notes: ¢ After installing an app press "Done" on the source device's screen (do not press "Open"). * Go back to the File manager screen after every installation so that you can install other required apps. ¢ In some devices you will prompted to grant "Install unknown apps" permissions in the File manager. CONTINUE 10. Manually install the APK file. Go to the File Manager [also called File Explorer, My Files, Mi File Manager etc.} on the source device and install the "Install_Me.apk" under All files or Storage. The icon of the app appears next to the "Install_Me.apk". 11. After installing the app, press Done on the source device's screen (do not press Open). 12. Go back to the File Manager screen after every installation so that you can install all the required apps. 13. Click Continue. You will be notified when to select Backup my data on the device to continue with the Android Backup process. For more information, see Android backup APK downgrade [on page 45). 4.4. Vendor backup 4.4.1. LG backup LG vendor backup allows you to extract user data that includes: » Personal data - contacts, text messages, call history, etc. » Media data - images. videos, audio, and documents » Installed applications data - LG settings, etc. This method supports all LG devices running on Android OS versions 5.x and higher. The extraction is first saved on the devices internal memory and then save on the target. De

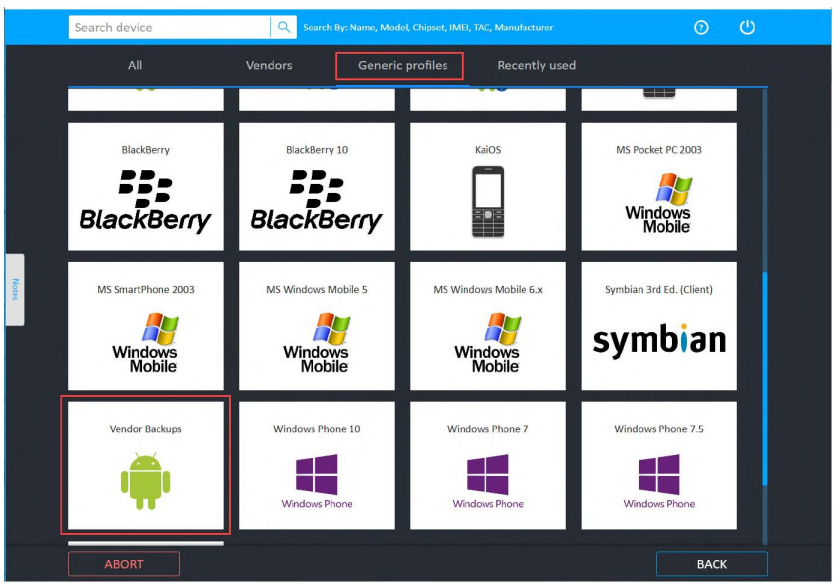
Manual installation required

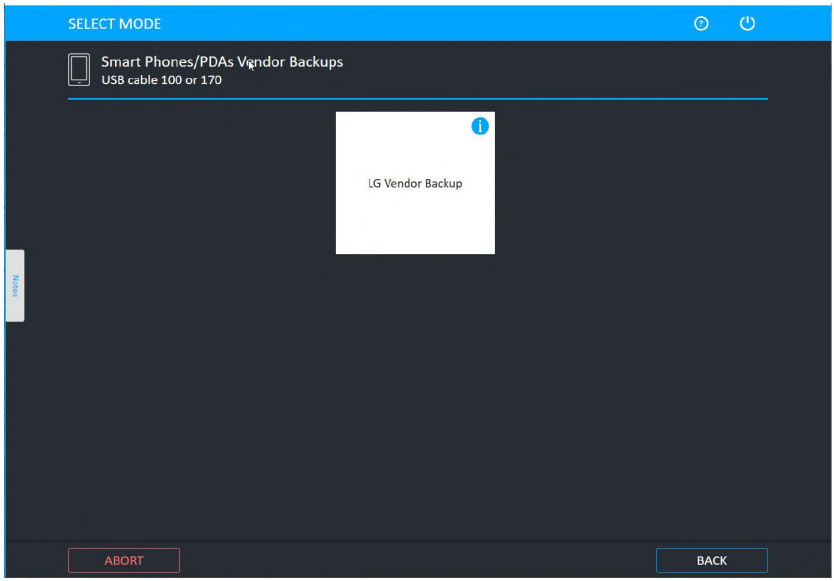
You need to manually install the app (APK file). Go to File manager (also called file explorer, my files etc.) and install the last APK file under All files/ storage called "Install_Me.apk".
These instructions are repeated twice for each app that requires manual installation (first the app is downgraded then the original app is restored).

Notes:
• After installing an app press "Done" on the source device's screen (do not press "Open").
• Go back to the File manager screen after every installation so that you can install other required apps.
• In some devices you will prompted to grant "Install unknown apps" permissions in the File manager.

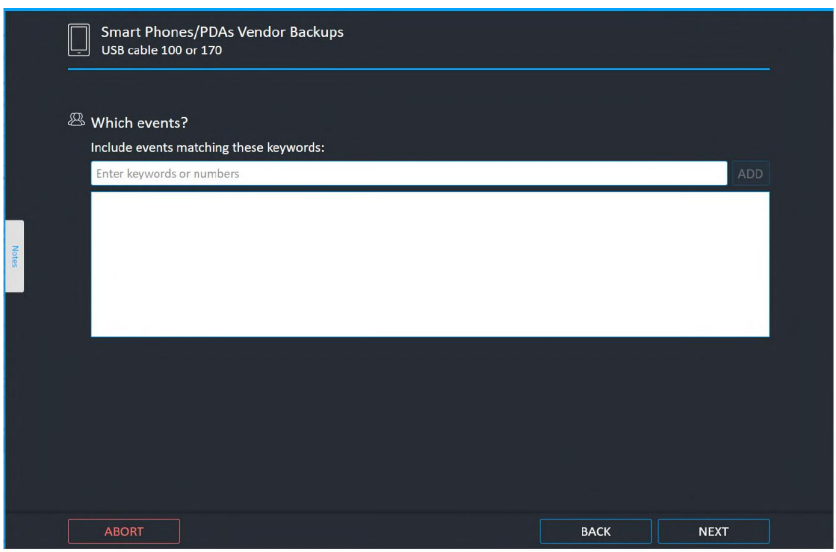
CONTINUE

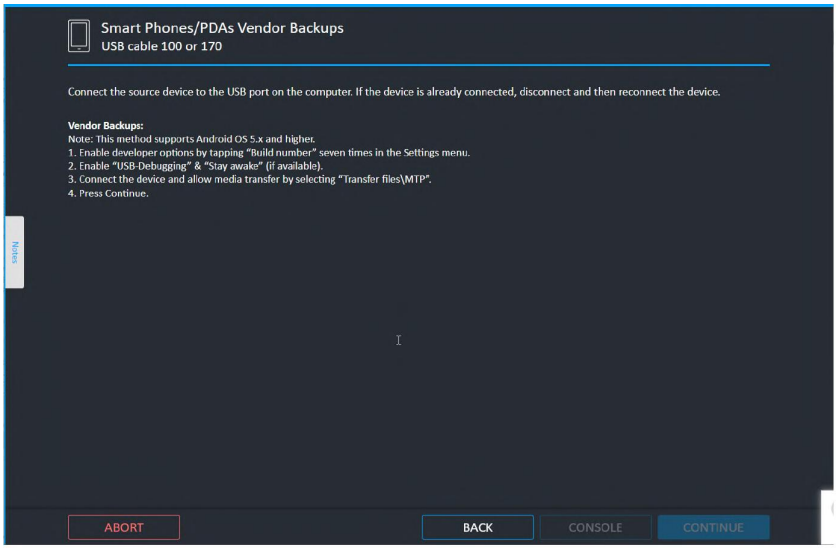
To extract data using LG backup: 1. Click on Mobile device. 2. Enter case details and click Continue. 3. Click Browse devices. 4. Under Generic profiles tab, select Vendor backups. © celebrite Responder 7360104 Search device Search By: Name, Model, Chipset, IMEI, TAC, Manufacturer Generic profiles Recently used MS Pocket PC 2003 ay BD BD ™ BlackBerry J BlackBerry Wiebe MS SmartPhone 2003 MS Windows Mobile 5 MS Windows Mobile 6.x Symbian 3rd Ed. (Client) ai P| a ae ag ag Windows Windows Windows Mobile Mobile Mobile symbian Vendor Backups Windows Phone 10 Windows Phone 7 Windows Phone 7.5 , ; ‘Windows Phone Windows Phone Windows Phone Click File system. Click LG vendor backup. © celebrite Responder 7360104 SELECT MODE Smart Phones/PDAs Vendor Backups USB cable 100 or 170 LG Vendor Backup 7. Enter keywords to include relevant events. Chapter 4: 04 Tn nn



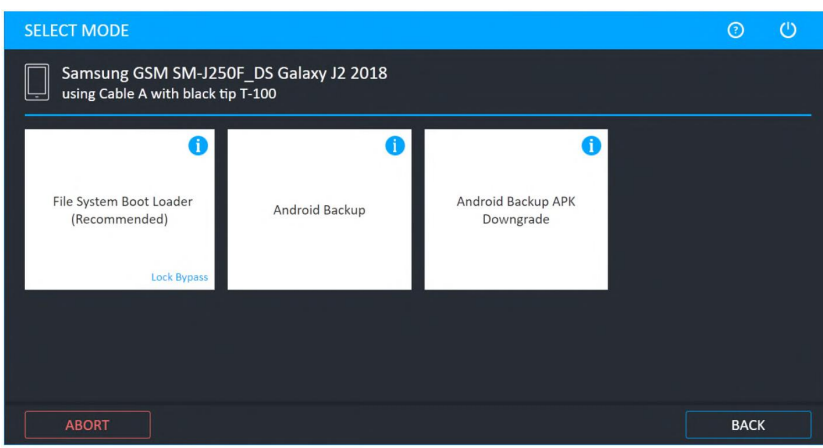

SELECT MODE
Smart Phones/PDAs Vendor Backups
USB cable 100 or 170
LG Vendor Backup
Notes
ABORT
BACK

Click Next. @ celebrite Responder 7360104 Smart Phones/ PDAs Vendor Backups USB cable 100 or 170 & Which events? Include events matching these keyword: Connect the device. @ celebrite Responder 7360104 Smart Phones/PDAs Vendor Backups USB cable 100 or 170 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. Vendor Backu Note: This method supports Android OS 5.x and higher. 1. Enable developer options by tapping “Build number” seven times in the Settings menu. 2. Enable “USB-Debugging” & “Stay awake” (if available). 3. Connect the device and allow media transfer by selecting “Transfer files\MTP”. 4. Press Continue. oo




Smart Phones/PDAs Vendor Backups
USB cable 100 or 170
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
Vendor Backups:
Note: This method supports Android OS 5.x and higher.
1. Enable developer options by tapping "Build number" seven times in the Settings menu.
2. Enable "USB-Debugging" & "Stay awake" (if available).
3. Connect the device and allow media transfer by selecting "Transfer files\MTP".
4. Press Continue.
Notes
ABORT
BACK
CONSOLE
CONTINUE

4.5. Selective file system extraction Selective extraction is part of the full file system extraction. It extracts all relevant app data located under the root directory. The app data includes folders and files associated with the app such as databases, APKs, images, and keys. Selective extraction takes less time to complete compared to a full file system extraction and enables you to only select the apps that are required. Selective extraction is currently supported for EDL Decrypting Bootloader, Samsung Qualcomm Decrypting Bootloader and Huawei Decrypting Bootloader methods. Selective extraction does not extract data from unallocated space. Use one of the Physical extraction methods instead. To extract data using Selective file system extraction: 1. Click Mobile device and identify the device, then click File System. SELECT MODE Samsung GSM SM-J250F_DS Galaxy J2 2018 using Cable A with black tip T-100 File System Boot Loader ‘ Android Backup APK Android Back (Recommended) nereeaenae Downgrade Lock Bypass 2. Click File System Boot Loader. For information on using optional timeframe and party filters, refer to the Overview Guide. 3. Select the extraction location. 4. Click Continue. The Waiting for Device screen appears. Chapter 4: 56 OO



UJ Samsung GSM SM-J250F_DS Galaxy J2 2018 using Cable A with black tip T-100 Connect the source device to the USB port he computer. If the device is already connected, disconnect and then reconnect the device. SM-J250F_DS Galaxy J2 2018: Note: This method is supported for OS versions up to and including To allow device connection: Note: The device battery should be fully charged. 1. Turn off the device. 2. Press and hold the Volume down, Home and Power buttons until the device enters Download mode. 3. Select “Continue” by pressing the Volume up button. 4 5. . Wait until the Download mode logo appears on the device screen, and then connect the device to the cable. . Connect the cable to UFED 4PC. 6. Select “Continue”. If a password is required to turn the device off, remove and re-insert the battery. If the device does not have a removable battery, perform the following steps: 1. Restart the device in Recovery mode: a. Restart the device by pressing the Power and Volume down buttons. When device restarts, quickly press and hold the Volume up, Home and Power buttons. b. When the device displays the Recovery mode screen, release the Volume up, Home and Power buttons. c. Wait for the Recovery menu to be displayed (this can take several minutes). 2. Select Power off, then press the Power button to turn off the device. Note: Use the Volume up and Volume down buttons to navigate the Recovery menu. 5. Connect the source device to the USB port. If the device is already connected, disconnect and then reconnect the device. 6. Click Continue. The following window appears. Huawei EVA-L19 P9 using USB cable 170 or Original Cable Please wait, this can take some time... Connecting The following window appears. 57

Samsung GSM SM-J250F_DS Galaxy J2 2018
using Cable A with black tip T-100

Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.

SM-J250F_DS Galaxy J2 2018:
Note: This method is supported for OS versions up to and including 7.1.1.
To allow device connection:
Note: The device battery should be fully charged.
1. Turn off the device.
2. Press and hold the Volume down, Home and Power buttons until the device enters Download mode.
3. Select "Continue" by pressing the Volume up button.
4. Wait until the Download mode logo appears on the device screen, and then connect the device to the cable.
5. Connect the cable to UFED 4PC.
6. Select "Continue".
If a password is required to turn the device off, remove and re-insert the battery.
If the device does not have a removable battery, perform the following steps:
1. Restart the device in Recovery mode:
a. Restart the device by pressing the Power and Volume down buttons. When the device restarts, quickly press and hold the Volume up, Home and Power buttons.
b. When the device displays the Recovery mode screen, release the Volume up, Home and Power buttons.
c. Wait for the Recovery menu to be displayed (this can take several minutes).
2. Select Power off, then press the Power button to turn off the device.
Note: Use the Volume up and Volume down buttons to navigate the Recovery menu.

ABORT | BACK | CONSOLE | CONTINUE

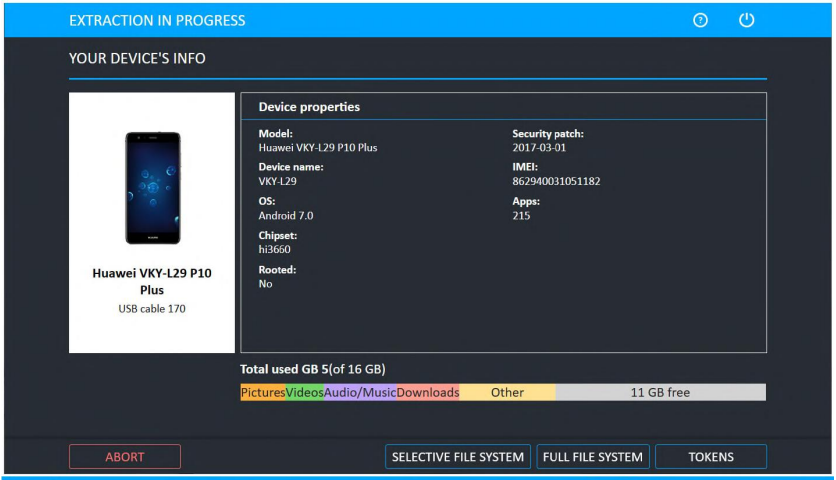
Huawei EVA-L19 P9
using USB cable 170 or Original Cable

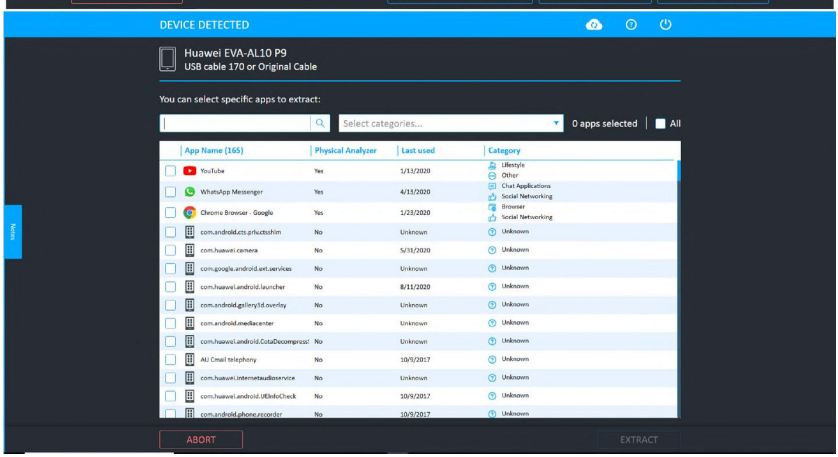
Please wait, this can take some time...

Connecting

ABORT

EXTRACTION IN PROGRESS YOUR DEVICE'S INFO Device properties Model: Security patch: Huawei VKY-L29 P10 Plus 2017-03-01 Device name: IMEI: VKY-L29 862940031051182 Os: Apps: Android 7.0 215 Chipset: hi3660 Huawei VKY-L29 P10 Rooted: No Plus USB cable 170 Total used GB 5(of 16 GB) 11 GB free SELECTIVE FILE SYSTEM | | FULL FILE SYSTEM TOKENS This window displays the device properties such as such as model, device name, OS, chipset, whether the device is rooted, date security patch installed, IMEA, and the number of installed apps, and what data Is on a device including storage volume, data types, volume of storage per data type, and free data. Click one of the following options: » Selective File System: The Selective extraction takes less time to complete and enables you to only select the required apps to extract. » Full File System: Full file system extraction including all apps and tokens. » Tokens: Retrieve data from cloud sources. Upon extraction and decoding, create the account package in Physical Analyzer and upload it into UFED Cloud. A Selective file system extraction example is displayed next. @ oo) - 9 x DEVICE DETECTED a Huawei EVA-AL10 P9 =} USB cable 170 or Original Cable You can select specific apps to extract: | App Name (165) | Physical Analyzer | Last used (1) > vourabe Yes 13/2020 {] @ whasapp messenger 4/13/2020 1/23/2020 Unknown s/ax/2oza Unknown 3/13/2020 Unknown Unknown Unkrown 10/9/2017 i ES Ba? Bas Ba ae: Unknown 20/9/2017 10/9/2017 7. Select the required apps and the click Extract. The Extraction Summary window appears. You can search for apps by category from the Select categories list. Chapter 4: 58


EXTRACTION IN PROGRESS
YOUR DEVICE'S INFO
Huawei VKY-L29 P10 Plus
USB cable 170
Device properties
Model:
Huawei VKY-L29 P10 Plus
Device name:
VKY-L29
OS:
Android 7.0
Chipset:
hi3660
Rooted:
No
Security patch:
2017-03-01
IMEI:
862940031051182
Apps:
215
Total used GB 5(of 16 GB)
Pictures
Videos
Audio/Music
Downloads
Other
11 GB free
ABORT
SELECTIVE FILE SYSTEM
FULL FILE SYSTEM
TOKENS

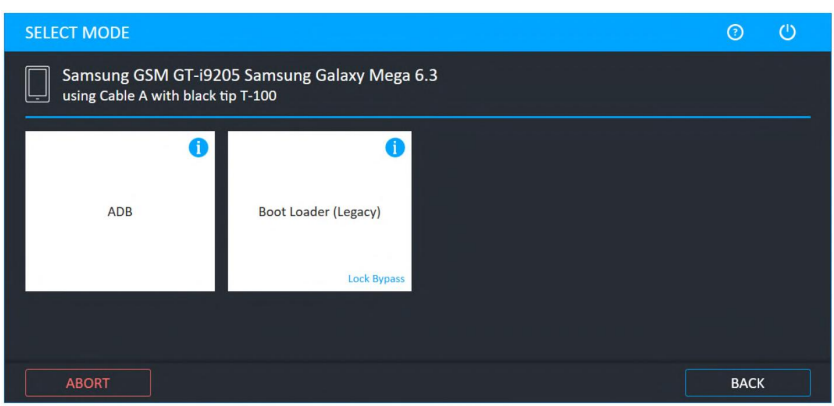

DEVICE DETECTED
Huawei EVA-AL10 P9
USB cable 170 or Original Cable
You can select specific apps to extract:
Select categories...
0 apps selected
All
App Name (165)
Physical Analyzer
Last used
Category
YouTube
Yes
1/13/2020
Lifestyle
Other
WhatsApp Messenger
Yes
4/13/2020
Chat Applications
Social Networking
Chrome Browser - Google
Yes
1/23/2020
Browser
Social Networking
com.android.cts.priv.ctsshim
No
Unknown
Unknown
com.huawei.camera
No
5/31/2020
Unknown
com.google.android.ext.services
No
Unknown
Unknown
com.huawei.android.launcher
No
8/11/2020
Unknown
com.android.gallery3d.overlay
No
Unknown
Unknown
com.android.mediacenter
No
Unknown
Unknown
com.huawei.android.CotaDecompress
No
Unknown
Unknown
AU Cmail telephony
No
10/9/2017
Unknown
com.huawei.internetaudioservice
No
Unknown
Unknown
com.huawei.android.UEInfoCheck
No
10/9/2017
Unknown
com.android.phone.recorder
No
10/9/2017
Unknown
ABORT
EXTRACT

9. Physical extraction The Physical Extraction function enables you to perform a physical bit-for-bit image of the source device memory to a removable storage device or PC. Physical extractions Include the following: Performing a physical extraction lon page 60) ADB rooted [on page 63) Advanced ADB [on page 65) Boot loader (FW flashing) [on page 82) Decrypting boot loader (on page 85) Forensic recovery partition (on page 87) Smart ADB [on page 91) UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/ Lock Bypass is displayed if the physical extraction method can bypass the user lock of the device. oY

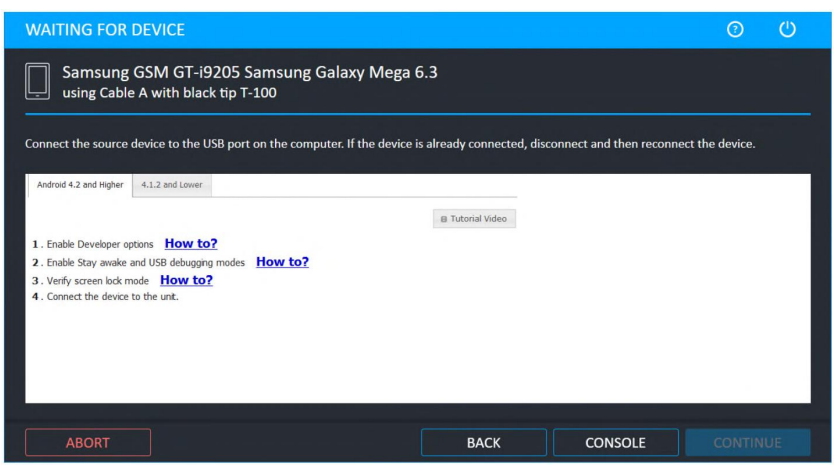
UFED now provides a notification if advanced forensic capabilities are available via Cellebrite Advanced Services for a growing range of supported Android and iOS devices. To learn more refer to: https://www.cellebrite.com/en/services/advanced-unlocking-services/

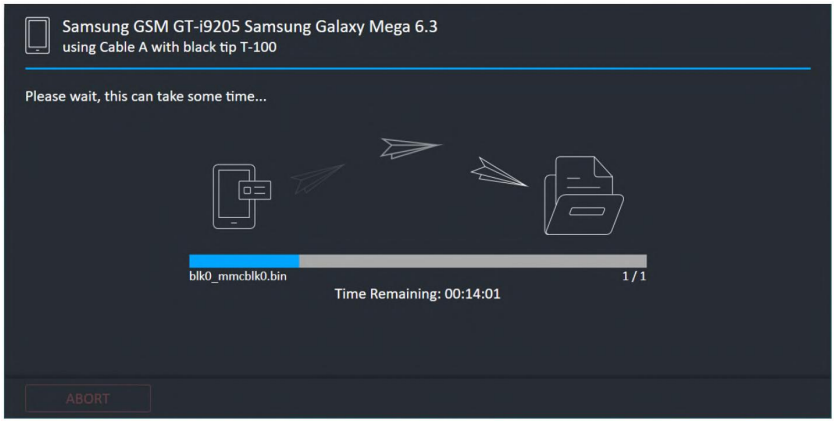
Lock Bypass is displayed if the physical extraction method can bypass the user lock of the device.

6.1. Performing a physical extraction 1. Click Mobile device and identify the device, then click Physical. The Select Mode screen appears. SELECT MODE (] Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Boot Loader (Legacy) 2. Click ADB or Boot Loader (Legacy). » ADB: Android Debug Bridge {ADB} is a built-in communication mechanism that allows device debugging. With this extraction method, it is possible to perform a physical or file system extraction, provided that the device's USB debugging option is enabled. If the device is not already rooted, UFED will attempt to temporarily gain the permissions required for the extraction. In some cases, data from a memory card will be extracted; however, the recommended method is to read the card with an external memory card reader. » Boot Loader: An extraction method that performs a physical extraction when the device is in bootloader mode. With this extraction, the operating system is not running, so the device cannot connect to the mobile network. It bypasses any user lock and is forensically sound. The bootloader extraction does not support extractions from a memory card. For information on using optional timeframe and party filters, refer to the Overview Guide. The Select Extraction Location screen appears. 3. Click Next. 60

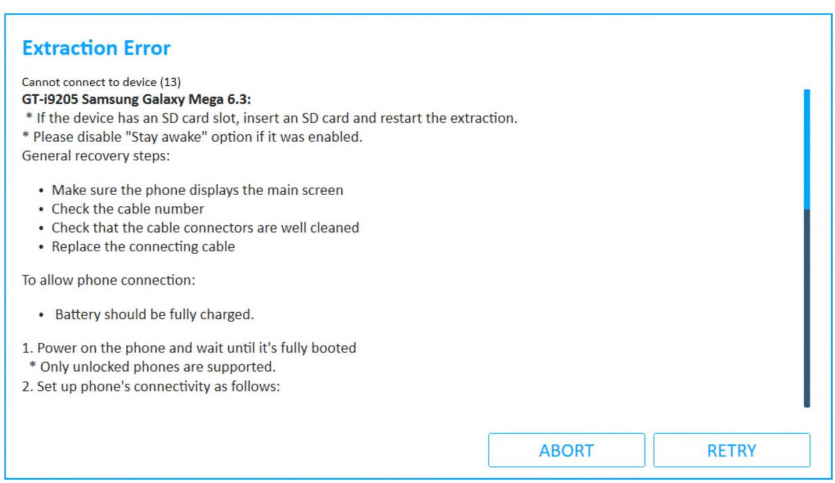


WAITING FOR DEVICE (] Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. Android 4.2 and Higher | 4.1.2 and Lower & Tutorial Video 1. Enable Developer options How to? 2. Enable Stay awake and USB debugging modes How to? 3. Verify screen lock mode How to? 4. Connect the device to the unit. CONSOLE 4. Do the following: » Select the correct cable and tip for the mobile device based on the instruction on the screen. » Change the device settings according to the instructions. 5. Click Continue. The Extraction in Progress screen appears. Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 Please wait, this can take some time... blkO_mmcblk0.bin Time Remaining: 00: 6. Follow any on-screen instructions. =i) For some devices, an estimation of the time the extraction will take is displayed: For example, Blackberry, Nokia BB5, QCP (SamM550, LgEmergency, LgP0), Android, (generic and SPF), SpreadTrum, Samsung GSM [MTK, LGInfinion, and BCM2133], and Palm. Chapter 6: 61 SSS ang a ea tt

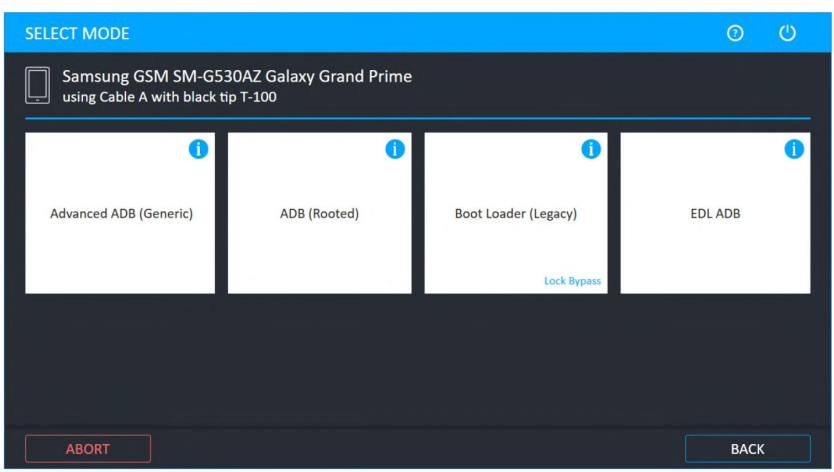

WAITING FOR DEVICE
Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
Android 4.2 and Higher
4.1.2 and Lower
Tutorial Video
1. Enable Developer options How to?
2. Enable Stay awake and USB debugging modes How to?
3. Verify screen lock mode How to?
4. Connect the device to the unit.
ABORT
BACK
CONSOLE
CONTINUE


Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3
using Cable A with black tip T-100
Please wait, this can take some time...
blk0_mmcblk0.bin
1 / 1
Time Remaining: 00:14:01
ABORT

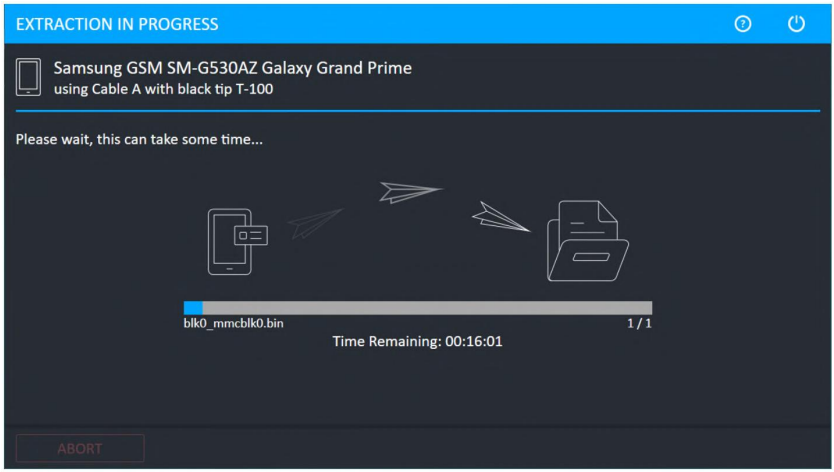
If the system cannot connect to the device: The following window appears with an error message. Extraction Error Cannot connect to device (13) GT-i9205 Samsung Galaxy Mega 6.3: * If the device has an SD card slot, insert an SD card and restart the extraction. * Please disable "Stay awake" option if it was enabled. General recovery steps: « Make sure the phone displays the main screen * Check the cable number * Check that the cable connectors are well cleaned « Replace the connecting cable To allow phone connection: * Battery should be fully charged. 1. Power on the phone and wait until it's fully booted * Only unlocked phones are supported. 2. Set up phone's connectivity as follows: » Follow the instructions on the screen and click Retry. 6.1.1. The Physical extraction folder At the end of the physical extraction process, the extracted data is saved in the location you selected during the physical extraction process. See step 5 of Performing a Physical Extraction. The extracted data folder is named “Physical” with the selected device name and the extraction operation date. For example, “Physical Samsung GSM SGH-A711 2011_06_12 (001)" The extracted data folder contains: » Binary file of the device memory. » UFD file containing the system extraction information, used by the Physical Analyzer application. The extraction information can be viewed using the Physical Analyzer. You can double click on the UDF file or open it via the GUI. 62


Extraction Error
Cannot connect to device (13)
GT-i9205 Samsung Galaxy Mega 6.3:
* If the device has an SD card slot, insert an SD card and restart the extraction.
* Please disable "Stay awake" option if it was enabled.
General recovery steps:
• Make sure the phone displays the main screen
• Check the cable number
• Check that the cable connectors are well cleaned
• Replace the connecting cable
To allow phone connection:
• Battery should be fully charged.
1. Power on the phone and wait until it's fully booted
* Only unlocked phones are supported.
2. Set up phone's connectivity as follows:
ABORT
RETRY

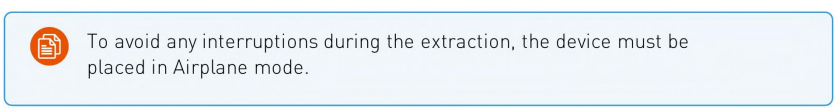
6.2. ADB rooted The ADB method for Android rooted devices can be used when the physical extraction method is not supported. Using the ADB method, you can perform a physical extraction from rooted Android devices. This extraction method is for pre-rooted devices only, and does not root the device. To “root” a device means to gain administrative rights on the file system. A device can be rooted as part of recovery partition or fully rooted following a rooting procedure. It does not suggest that you should root the device, however, if there is no other option, you can use this method. To perform a physical extraction for a rooted Android device: 1. Click Mobile device and identify the device, then click Physical. The Select Mode screen appears: SELECT MODE Samsung GSM SM-G530AZ Galaxy Grand Prime using Cable A with black tip T-100 Advanced ADB (Generic) ADB (Rooted) Boot Loader (Legacy) EDL ADB 2. Click ADB (Rooted). For information on using optional timeframe and party filters, refer to the Overview Guide. The Select Extraction Location screen appears. 3. Click Next. The following window appears. 4. Do the following: » Select the correct cable and tip for the mobile device based on the instruction on the screen. » Change the device settings according to the instructions. 5. Click Continue. Chapter 6: 63 SSS a a ttt



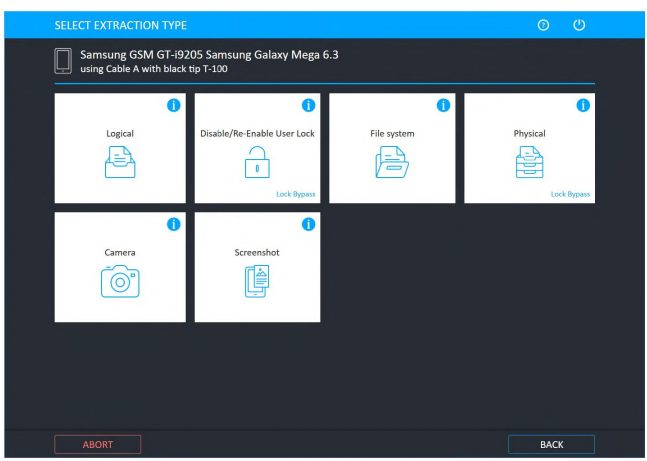
The Extraction in Progress screen appears. EXTRACTION IN PROGRESS (J Samsung GSM SM-G530AZ Galaxy Grand Prime using Cable A with black tip T-100 Please wait, this can take some time... F blkO_mmcblk0.bin Time Remaining: 00:16:01 6. Follow any on-screen instructions. 64



6.3. Advanced ADB Advanced ADB extraction enables physical extraction of data from additional devices. This method supports devices with Android operating systems up to version 7.1, on devices with a security patch level up to November 2016, including Galaxy S7, Galaxy Note 5, LG G5, V20, and Nexus devices. Due to the widely fragmented variance in Android devices, exceptions may apply. To avoid any interruptions during the extraction, the device must be placed in Airplane mode. Before performing an Advanced ADB extraction: 1. Make sure the source device Is fully charged. 2. Prepare a target storage device on which to save the extraction file. This target can be either a USB mass storage device {connected via OTG cable 501 or 508), or an SD memory card. » The target storage device must be a FAT32/vFAT/ exFAT format and have sufficient space for the extraction. » Ifa USB drive is selected for the target storage, make sure you have an available OTG cable for the extraction: OTG cable 501 (micro USB connector] or cable 508 (type C connector]. OTG cable example: a —— nT » Ifan SD card is selected for the target storage, place it in the Android device now. The SD card must be blank and not contain any case evidence. If the card port location is under the device's battery, restarting may re-lock a device that was locked before. Therefore, for devices with OTG support, we recommend using a USB drive for the target storage. Chapter 6: 65 nn

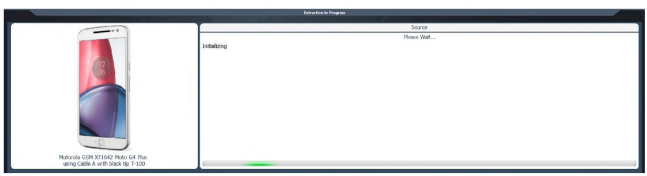


To perform an Advanced ADB extraction: 1. From the Home screen, detect the relevant device automatically. The following window appears. SELECT EXTRACTION TYPE Oj Samsung GSM GT-i9205 Samsung Galaxy Mega 6.3 using Cable A with black tip T-100 fi) Logical Disable/Re-Enable User Lock File system Physical e | = Camera Screenshot E If the relevant modelis not listed, browse manually for a generic Android model. See Generic model (on page 73). 2. Click Physical. The Select Mode screen appears. 3. Click Advanced ADB. For information on using optional timeframe and party filters, refer to the Overview Guide. 4. Follow the instructions to set up device connectivity. 5. On the source device, perform the following steps: a. OnanAndroid OS 4.3 and above, Go to Menu (Apps) > Settings (More) > Security and clear the Verify apps setting. Approve any pop-ups that may appear. b. Go to Menu (Apps) > Settings (More) > About (Software information) > More, and tap the Build number 7 times until developer options are enabled. c. Go to Development settings and enable USB debugging. d. Connect the source device to the cable described in UFED. e. A notification is added to the notification drop down. Allow MTP/PTP on the device. 66



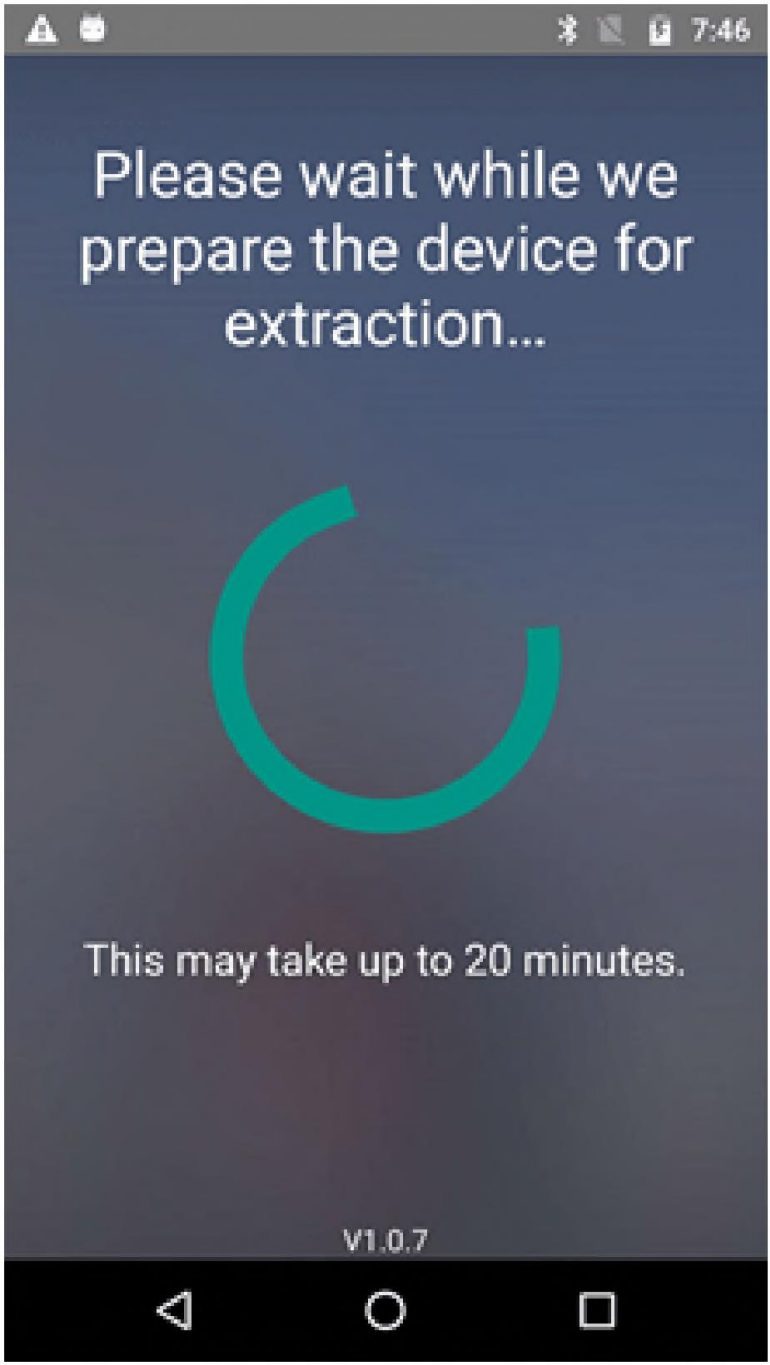
If the relevant model is not listed, browse manually for a generic Android model. See Generic model (on page 73).

6. On the UFED screen, click Continue. The following window appears. Warning Before you select the target storage: If the target storage is an SD card, place it in the device now. Reminder: Restarting may re-lock the device. For this reason a USB drive is recommended for the target storage. If the target device is not recognized by the Android device click "Help with storage format" | SD. CARD WASINSERTED _ || MASS STORAGE | | HELP WITH STORAGE FORMAT 7. Click the relevant target storage. The following window appears. Motorola GSM XT1642 Moto G4 Plus using Cable A with black tip T-100 b =i) 'f requested, you should only approve the installation of apps. Chapter 6: 67

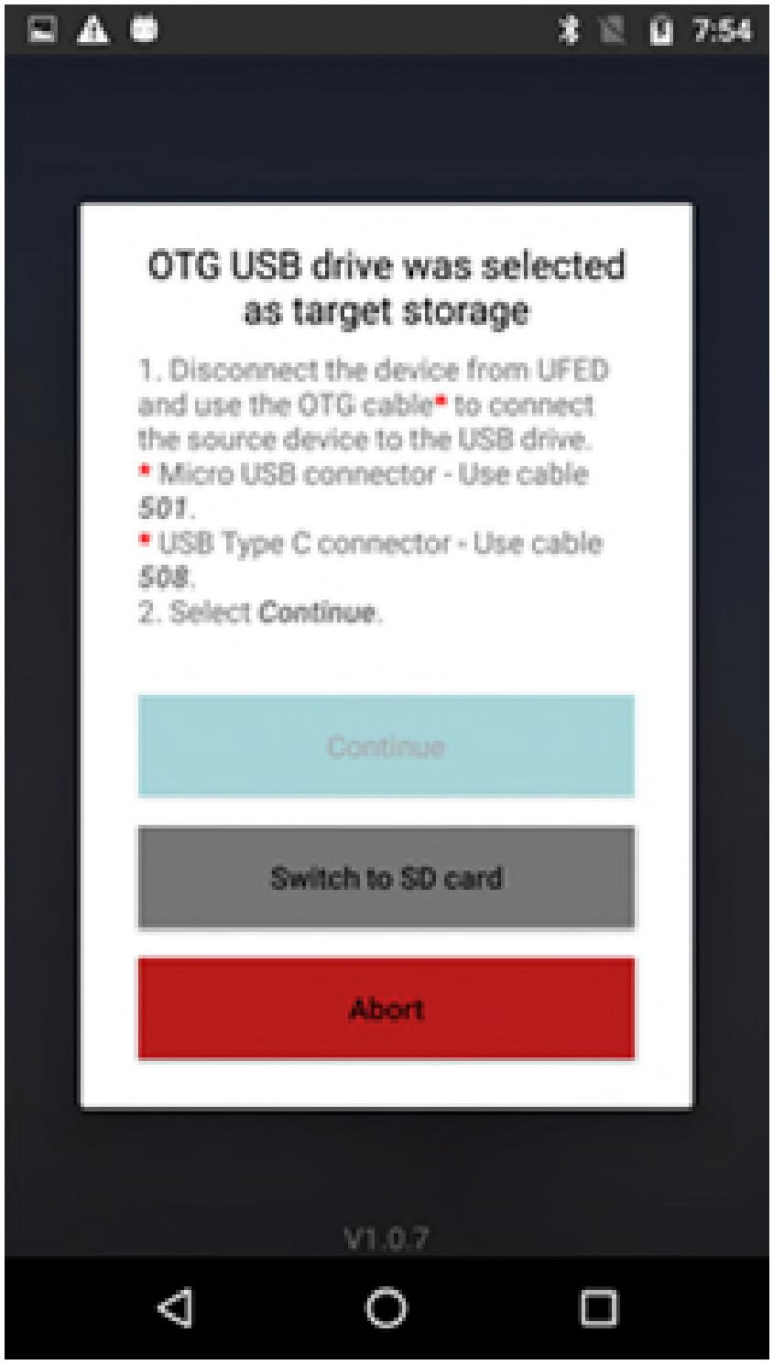


If requested, you should only approve the installation of apps.

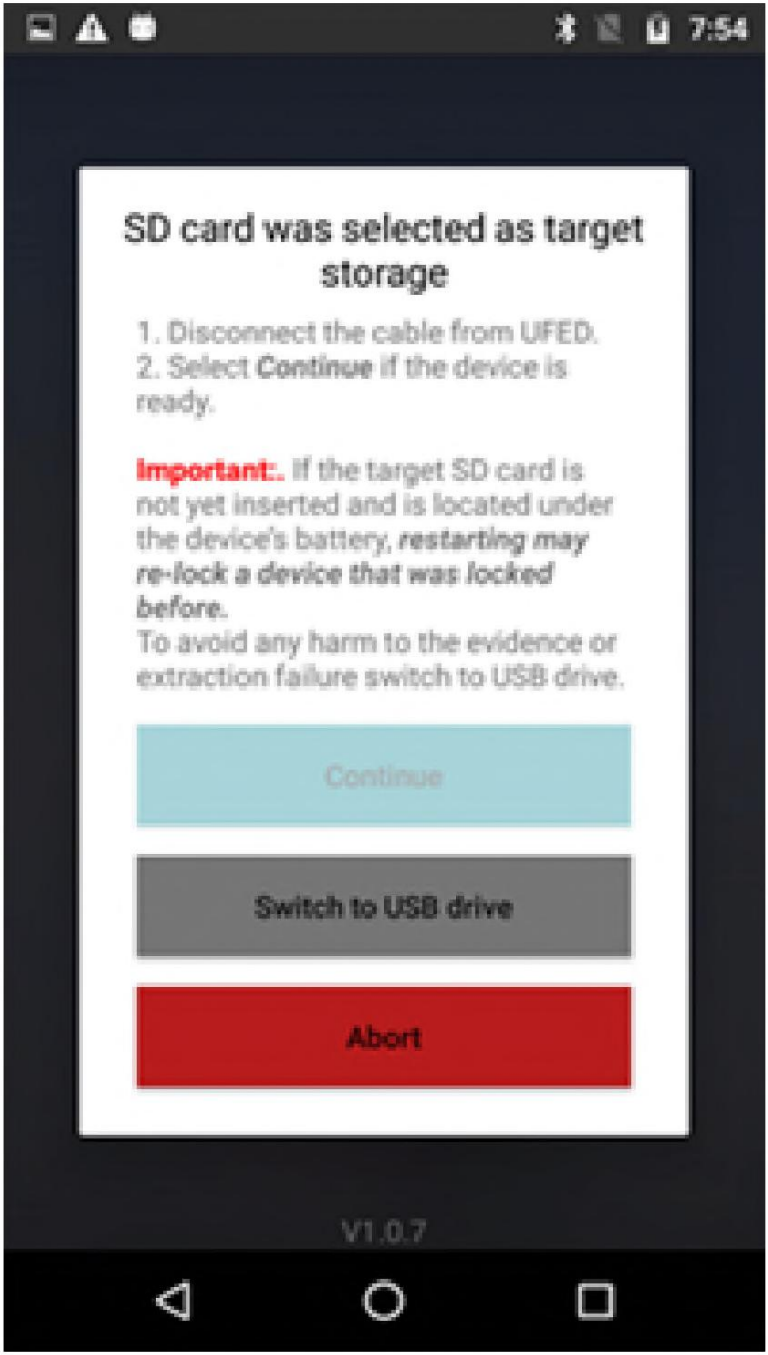
UFED is installing the extraction app and attempting to temporarily gain the permissions required for the extraction. This stage can take approximately 20 minutes. During this process, the device screen appears. A 8 i 746 Please wait while we prepare the device for extraction... This may take up to 20 minutes. When UFED has prepared the device, a window appears Indicating that the device Is ready for extraction. Disconnect the device from UFED and follow the instructions on the source device. 8. Click Continue. 9. Follow the instructions on the Android source device's screen. For a USB drive target, continue to the following step. For an SD card target, skip to the next step. 68


7:46
Please wait while we prepare the device for extraction...
This may take up to 20 minutes.
V1.0.7

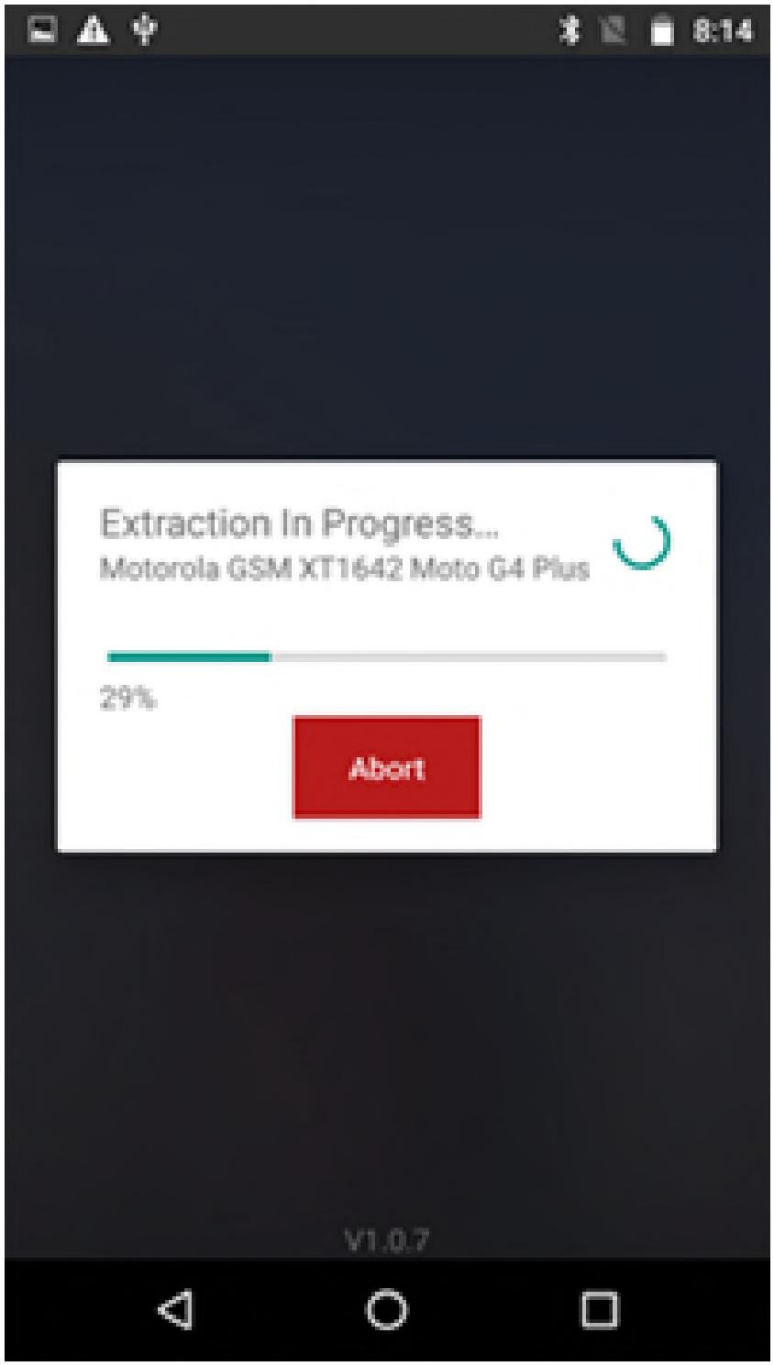
10. If a USB drive target was selected, the following screen appears. OTG USS drive was selected as target storage a. Follow the on-screen instructions: i. Disconnect the device from UFED. ii. Use the OTG cable to connect the source device to the USB drive. Selecting Switch to SD card will change the target type configuration. Selecting Abort will end the extraction process and will require a device restart. b. Skip the SD card step. c. lfan SD card target was selected, the following screen appears. Chapter 6: 69 SSS an a ttt


7:54
OTG USB drive was selected as target storage
1. Disconnect the device from UFED and use the OTG cable* to connect the source device to the USB drive.
* Micro USB connector - Use cable 501.
* USB Type C connector - Use cable 508.
2. Select Continue.
Continue
Switch to SD card
Abort
V1.0.7

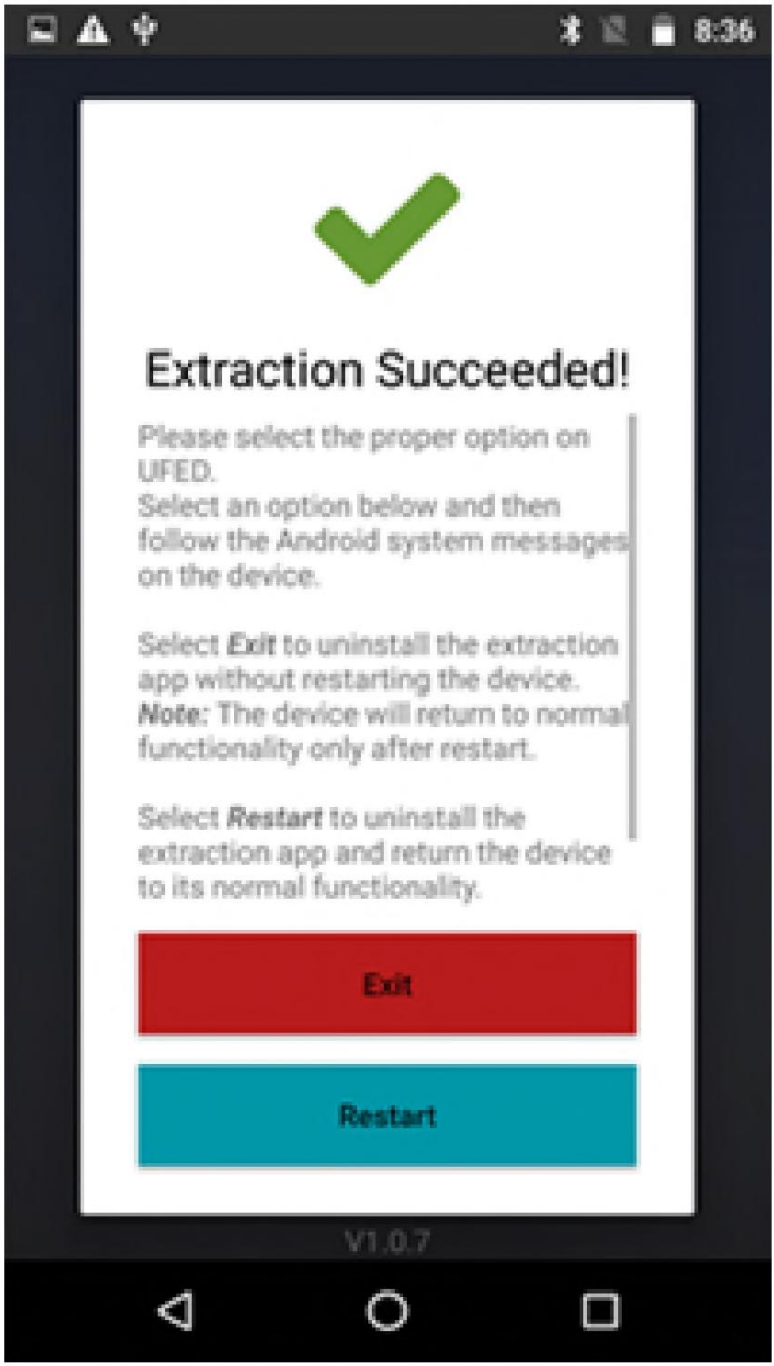
50 card was selected as tanget storage a. Follow the on-screen instructions: i. Disconnect the device from UFED. il. Ifthe target SD card is not yet inserted and is located under the device's battery, restarting may re-lock a device that was locked before. To avoid an extraction failure (for devices with OTG support], select Switch to USB drive. Reminder: This target device requires A FAT32*/vFAT/exFAT format SD card with sufficient space for the extraction. Selecting Switch to USB drive will change the target type configuration. Selecting Abort will end the extraction process and will require a device restart. 70


7:54
SD card was selected as target storage
1. Disconnect the cable from UFED.
2. Select Continue if the device is ready.
Important:. If the target SD card is not yet inserted and is located under the device's battery, restarting may re-lock a device that was locked before.
To avoid any harm to the evidence or extraction failure switch to USB drive.
Continue
Switch to USB drive
Abort
V1.0.7

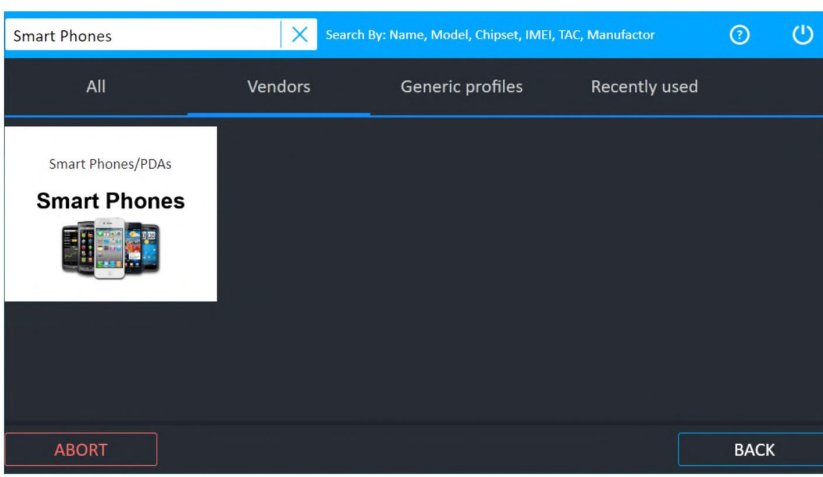
12. Select Continue. The reading process begins. When the extraction is successfully completed, the following screen appears.
Chapter 6: 71 ee

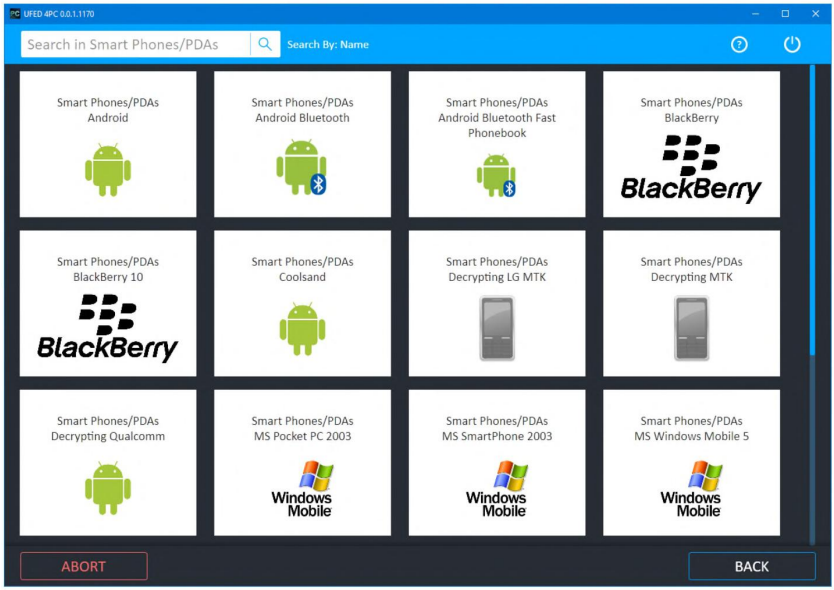

8:14
Extraction In Progress...
Motorola GSM XT1642 Moto G4 Plus
29%
Abort
V1.0.7

Extraction Succeeded! < q O O 13. Select Exit to uninstall the extraction app without restarting the device, or select Restart to uninstall the extraction app and return the device to its normal functionality. Restarting may re-lock a device that was locked before. The device will only return to normal functionality after restart. 14. Return to UFED. 15. Follow the on-screen instructions on the source device. When the extraction completes click Extraction failed, Extraction successful or Abort to update the extraction Activity log. oO Click the relevant extraction status to update the extraction Activity log. 17. Follow the instructions and click Finish.

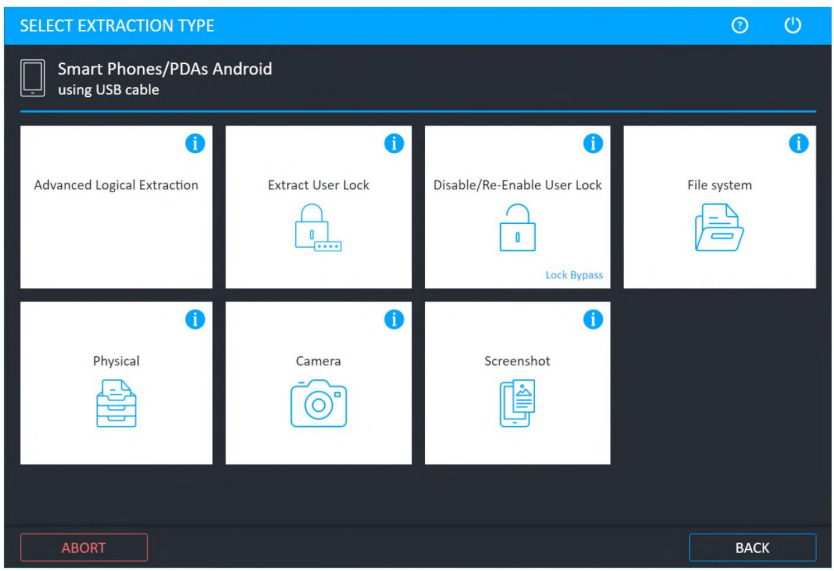

8:36
Extraction Succeeded!
Please select the proper option on UFED.
Select an option below and then follow the Android system messages on the device.
Select Exit to uninstall the extraction app without restarting the device.
Note: The device will return to normal functionality only after restart.
Select Restart to uninstall the extraction app and return the device to its normal functionality.
Exit
Restart
V1.0.7

6.3.1. Generic model To perform an Advanced ADB extraction: 1. From the Home screen, click Skip > Vendors [tab] and search for "Smart Phones". The following window appears. Smart Phones | X< Search By: Name, Model, Chipset, IMEI, TAC, Manufactor All Smart Phones/PDAs Smart Phones 2. Click Smart Phones. Smart Phones/PDAs Android Smart Phones/PDAs BlackBerry 10 p>» BlackBerry Smart Phones/PDAs Decrypting Qualcomm im (ry! Chapter 6: Vendors The following window appears. [OM Search By: Name Smart Phones/PDAs Android Bluetooth Smart Phones/PDAs Coolsand rN iy! Smart Phones/PDAs MS Pocket PC 2003 fe ae Windows Mobile Generic profiles Smart Phones/PDAs Android Bluetooth Fast Phonebook Smart Phones/ PDAs Decrypting LG MTK Smart Phones/PDAs MS SmartPhone 2003 fe ae Windows Mobile Recently used Smart Phones/PDAs BlackBerry ap» BlackBerry Smart Phones/PDAs Decrypting MTK Smart Phones/PDAs MS Windows Mobile 5 a au Windows Mobile ie

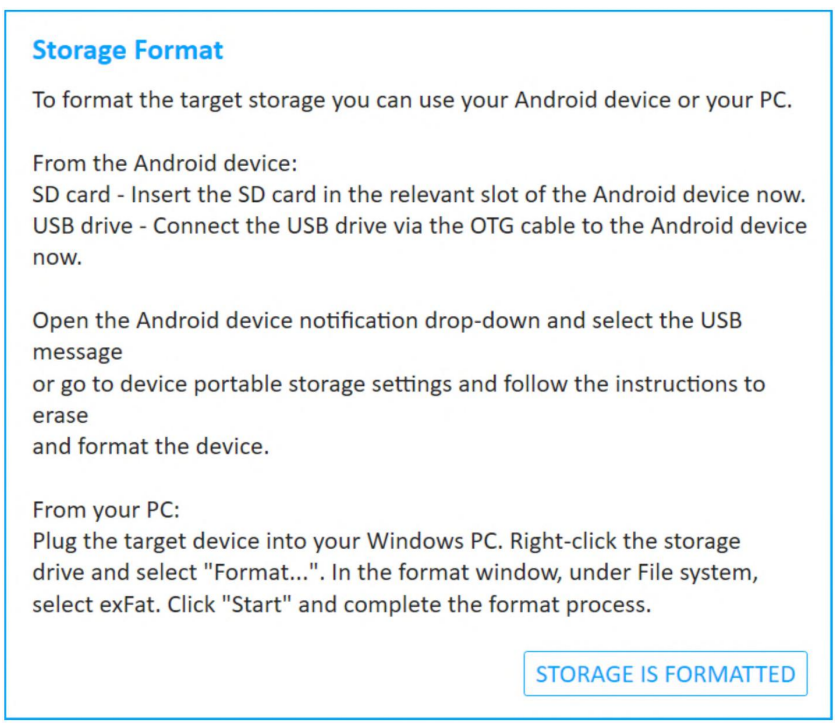



UFED 4PC 0.0.1.1170
Search in Smart Phones/PDAs
Search By: Name
Smart Phones/PDAs Android
Smart Phones/PDAs Android Bluetooth
Smart Phones/PDAs Android Bluetooth Fast Phonebook
Smart Phones/PDAs BlackBerry
BlackBerry
Smart Phones/PDAs BlackBerry 10
BlackBerry
Smart Phones/PDAs Coolsand
Smart Phones/PDAs Decrypting LG MTK
Smart Phones/PDAs Decrypting MTK
Smart Phones/PDAs Decrypting Qualcomm
Smart Phones/PDAs MS Pocket PC 2003
Windows Mobile
Smart Phones/PDAs MS SmartPhone 2003
Windows Mobile
Smart Phones/PDAs MS Windows Mobile 5
Windows Mobile
ABORT
BACK

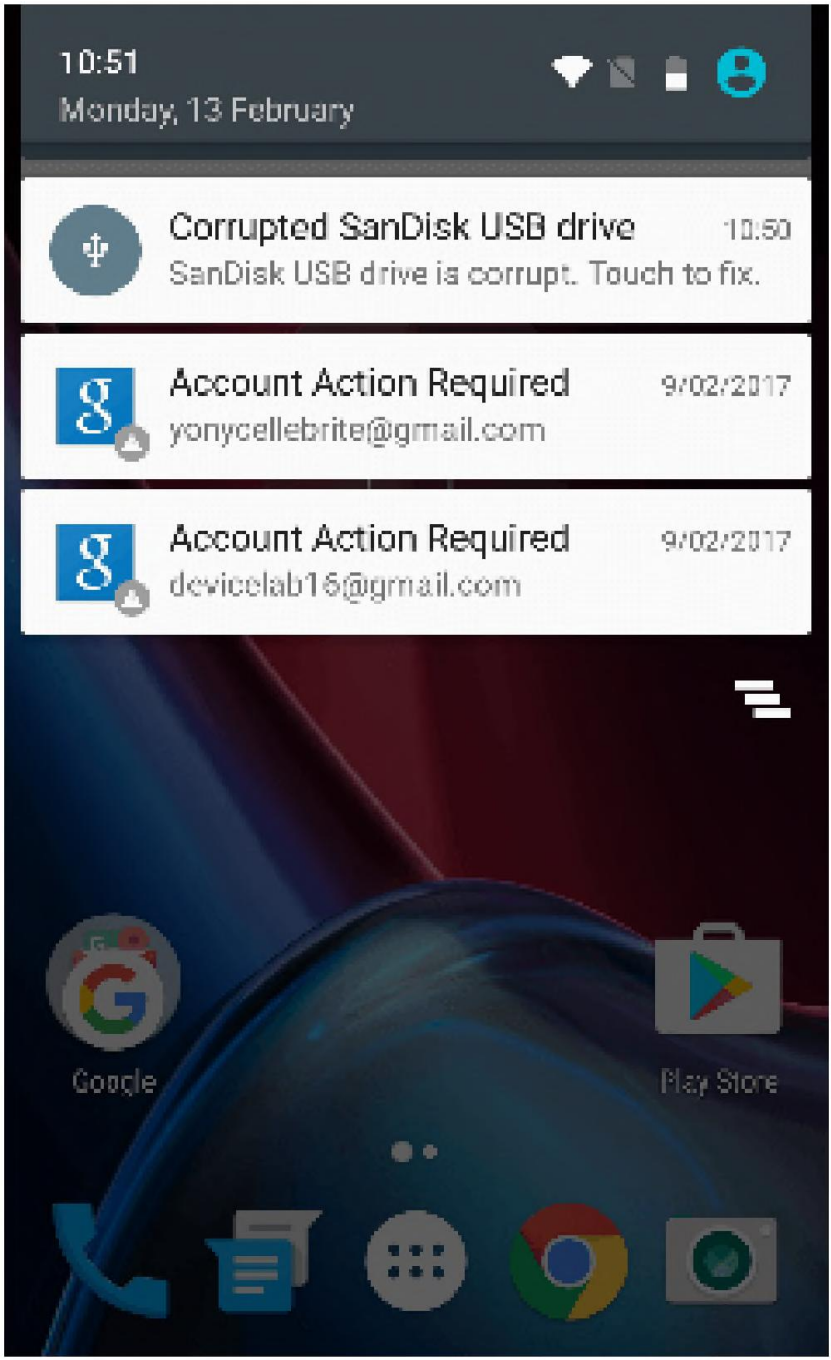
3. Click the relevant model. The following window appears. SELECT EXTRACTION TYPE Smart Phones/PDAs Android using USB cable Advanced Logical Extraction Extract User Lock Disable/Re-Enable User Lock Gy Lock Bypass Physical = 4. Click Physical. 5. To continue, refer to Advanced ADB [on page 65). File system 74



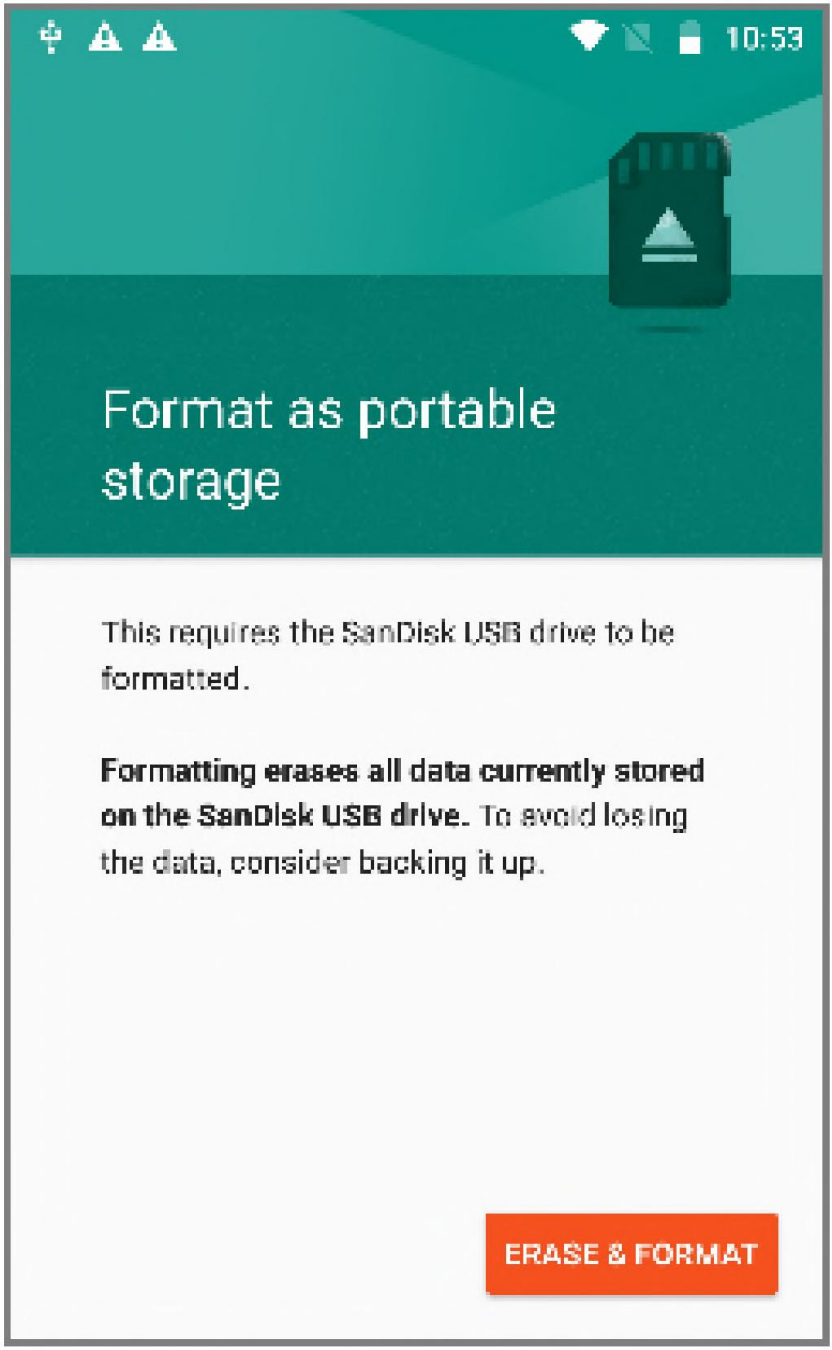
6.3.2. Errors and notifications 6.3.2.1. Disk format error Storage Format To format the target storage you can use your Android device or your PC. From the Android device: SD card - Insert the SD card in the relevant slot of the Android device now. USB drive - Connect the USB drive via the OTG cable to the Android device now. Open the Android device notification drop-down and select the USB message or go to device portable storage settings and follow the instructions to erase and format the device. From your PC: Plug the target device into your Windows PC. Right-click the storage drive and select "Format...". In the format window, under File system, select exFat. Click "Start" and complete the format process. STORAGE IS FORMATTED If you receive this error message, follow the instructions listed In the error message. Chapter 6: 7D ee


Storage Format
To format the target storage you can use your Android device or your PC.
From the Android device:
SD card - Insert the SD card in the relevant slot of the Android device now.
USB drive - Connect the USB drive via the OTG cable to the Android device now.
Open the Android device notification drop-down and select the USB message
or go to device portable storage settings and follow the instructions to erase
and format the device.
From your PC:
Plug the target device into your Windows PC. Right-click the storage drive and select "Format...". In the format window, under File system, select exFat. Click "Start" and complete the format process.
STORAGE IS FORMATTED

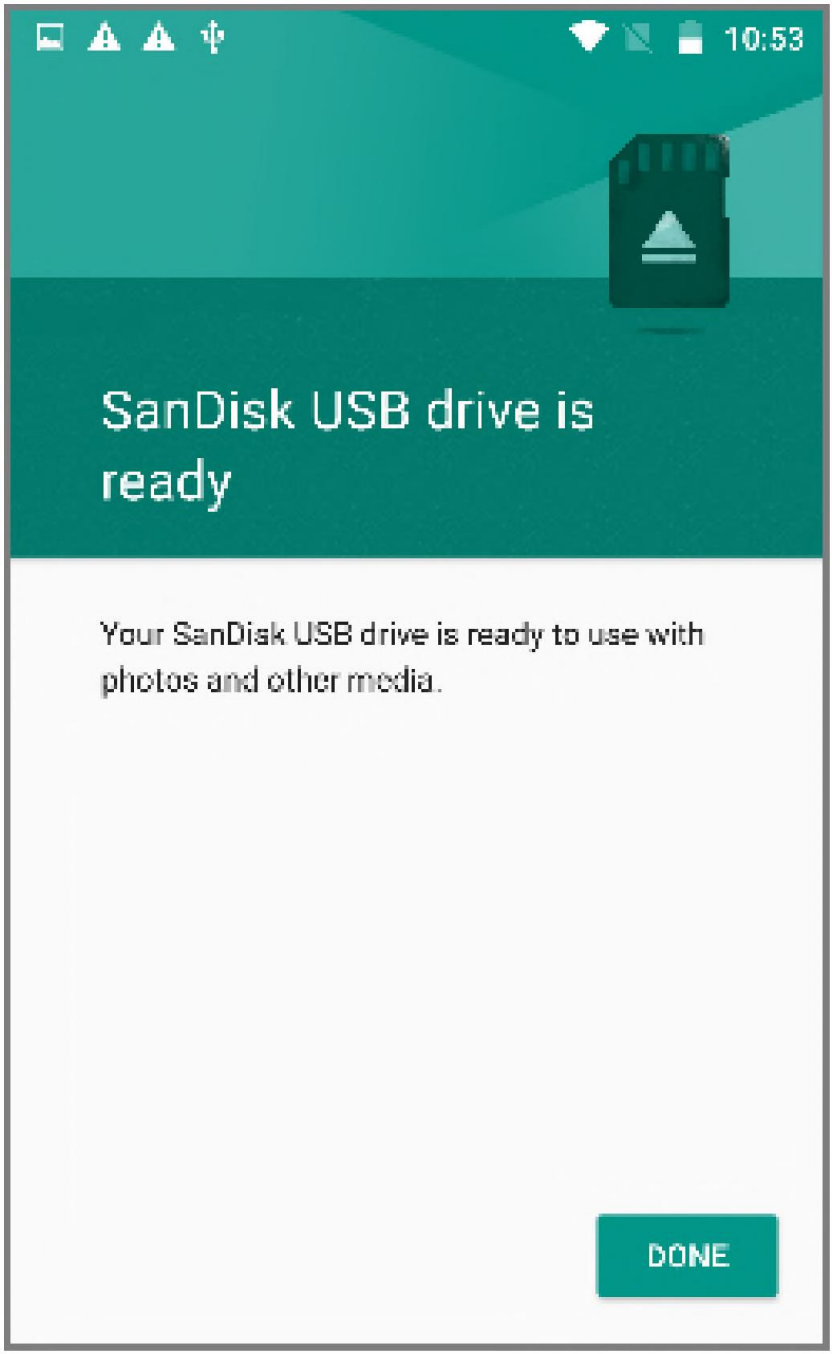
To format the storage device from the Android device: 1. Open notification. 10:57 Manda, 12 February Corrupted Sanbisk USB drive 10:50 SanDisk USE drive ia corrupt. Touch to fie. Account Action Required yanycellebrite mgm ail.com Account Action Required deviechal] Sagrnaileen 2. Select the Corrupted USB drive notification. The following screen appears. 76


10:51
Monday, 13 February
Corrupted SanDisk USB drive
10:50
SanDisk USB drive is corrupt. Touch to fix.
Account Action Required
9/02/2017
yonycellebrite@gmail.com
Account Action Required
9/02/2017
devicelab16@gmail.com
Google
Play Store

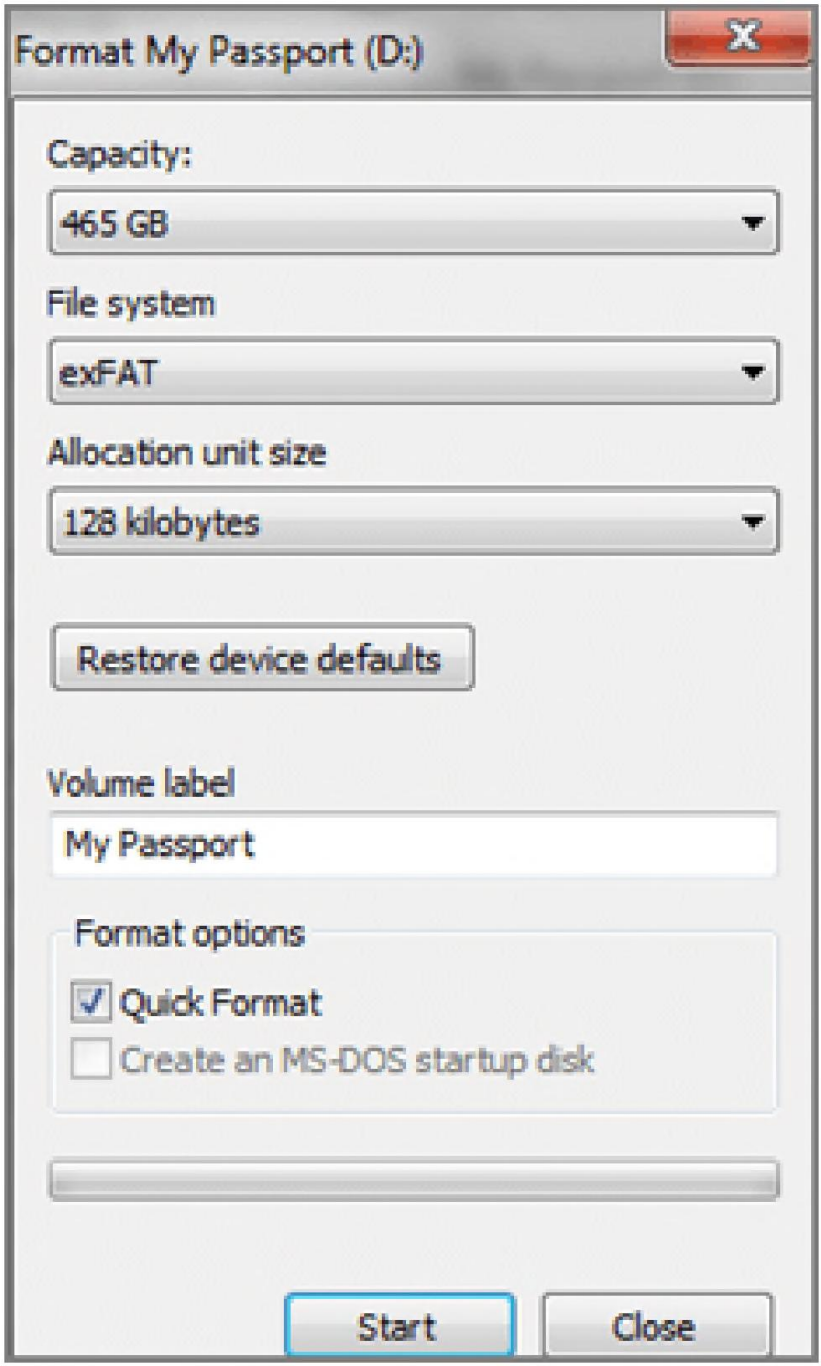
Format as portable storage This requires the Sanbisk US drive te be formatted. Formatting erases all data curently stored on the SanBlek USB drive. To evel losing the data, consider backing it up. ERASE & FORKLAT 3. Follow the instructions to erase and format the device. Upon completion, the following screen appears. Chapter 6: 77 ee


10:53
Format as portable storage
This requires the SanDisk USB drive to be formatted.
Formatting erases all data currently stored on the SanDisk USB drive. To avoid losing the data, consider backing it up.
ERASE & FORMAT

SanDisk USB drive is ready Your SanDisk USE drive is ready to use with photos ard other media. 78


10:53
SanDisk USB drive is ready
Your SanDisk USB drive is ready to use with photos and other media.
DONE

To format the storage device from the PC: 1. Plug the hard drive into your Windows PC. Right-click on the D drive and select “Format” The following window appears. 2. Under File System, select exFAT. 3. Click Start and complete the format process. Chapter 6: 79 ee

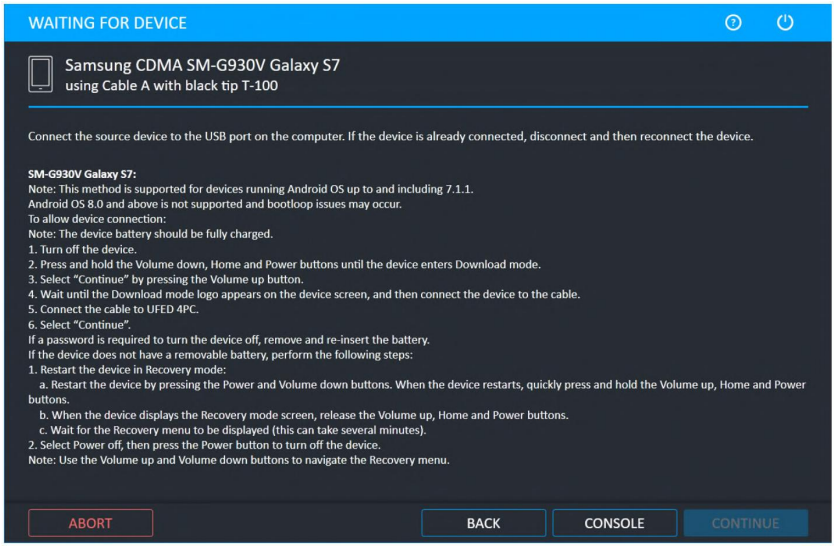

Format My Passport (D:)
Capacity:
465 GB
File system
exFAT
Allocation unit size
128 kilobytes
Restore device defaults
Volume label
My Passport
Format options
Quick Format
Create an MS-DOS startup disk
Start
Close

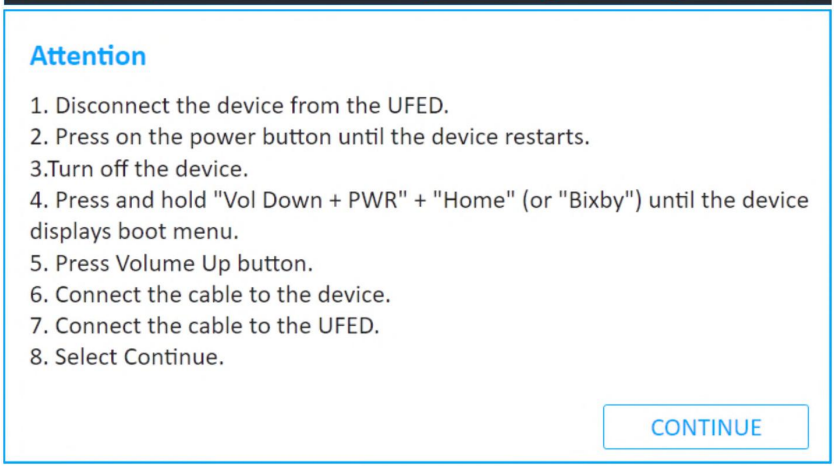
6.3.2.1.1. Extraction aborted lf Abort was selected during the extraction process, the screen on the left will appear. After some time (up to a few minutes] the screen on the right will appear. (x) Extraction aborted.. Extraction Aborted... Select an option below and then follow the Android system messages on the device. Aborting Please wait..this can take a few minutes. Select Exit to uninstall the extraction app without restarting the device. Note: The device will return to normal functionality only after restart. Select Restart to uninstall the extraction app and return the device to its normal functionality. Note: Restarting may re-lock a Gevice that was locked before. » Select Exit to uninstall the extraction app without restarting the device. The device will only return to normal functionality after restart. » Select Restart to uninstall the extraction app and return the device to its normal functionality. Restarting may re-lock a device that was locked before. 80

6.3.2.1.2. Extraction failed If the extraction failed for any reason, the following screen appears with the failure reason. Extraction failed tren: Your 5D card it not the night format fh this goctracton., The Storage Gevice must FATS2/vEATfexPAT format. Select an option below and then follow the Android system messages on the device. Select Bart 86 uranatall the aatrection app without restarting the darvice, Note: The device wall returnn to normal func enhy after hercert. Sehect Restart to urinatall the extraction & ane return the device te its monmal functionality, Note: Restarting may re-lock o device that was locked before, Ext » Select Exit to uninstall the extraction app without restarting the device. The device will only return to normal functionality after restart. » Select Restart to uninstall the extraction app and return the device to its normal functionality. Restarting may re-lock a device that was locked before. Chapter 6: 81 SSS a ttt

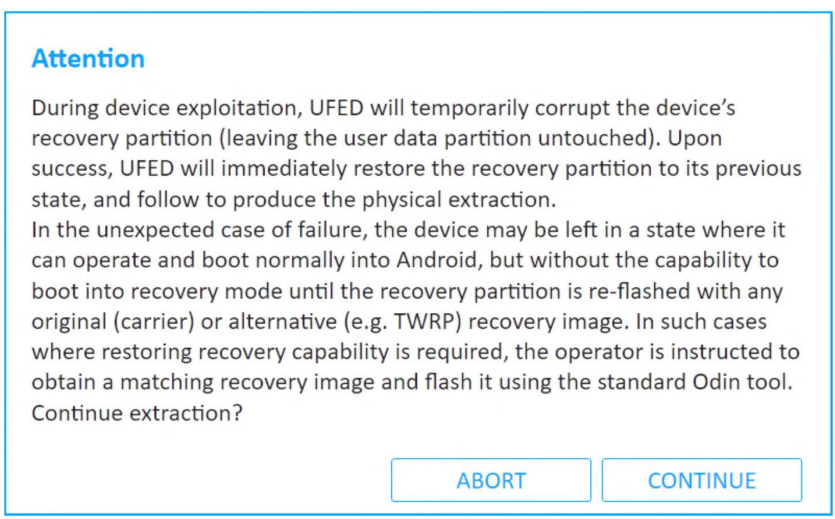
6.4. Boot loader (FW flashing) The Boot loader (FW flashing) extraction method uses boot loader reflashing, which enables a physical extraction while bypassing user lock {non-secure startup]. This method is for Qualcomm-based Samsung Galaxy S7 devices running firmware version of Android 7.x. Fora complete list of supported devices, refer to UFED Supported Devices document in MyCellebrite. This extraction does not support extractions from a memory card. This Boot loader (FW flashing} extraction method requires the device's firmware to be flashed. In some cases the device may experience unexpected behavior and you will need to flash the original device firmware, which causes a device wipe. Before using this method, we recommend trying other Physical bootloader methods. To perform Boot loader (FW flashing): 1. Click Mobile device and identify the device, then click Physical. The Select Mode screen appears: SELECT MODE (J Samsung CDMA SM-G930V Galaxy S7 using Cable A with black tip T-100 Boot Loader D ting EDL ADB (Recommended) SENPRDE Boot Loader (FW Flashing) Lock Bypass Lock Bypass 2. Select Boot loader (FW Flashing). For information on using optional timeframe and party filters, refer to the Overview Guide. The following Select extraction location window appears. 3. Select the extraction location. The Waiting for Device screen appears. 82

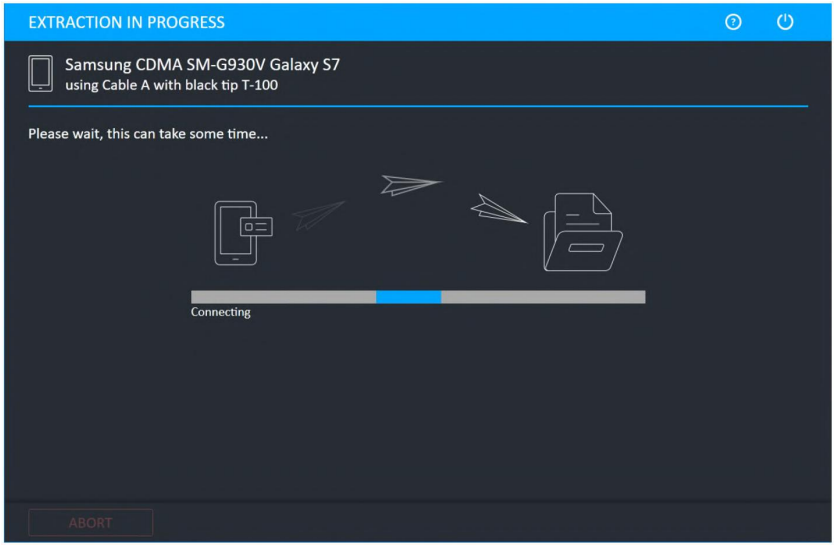
WAITING FOR DEVICE Samsung CDMA SM-G930V Galaxy S7 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. SM-G930V Galaxy S7: Note: This method is supported for devices running Android OS up to and including 7.1.1. Android OS 8.0 and above is not supported and bootloop issues may occur. To allow device connection: Note: The device battery should be fully charged. 1. Turn off the device. 2. Press and hold the Volume down, Home and Power buttons until the device enters Download mode. 3. Select “Continue” by pressing the Volume up button. 4. Wait until the Download mode logo appears on the device screen, and then connect the device to the cable. 5. Connect the cable to UFED 4PC. 6. Select “Continue”. If a password is required to turn the device off, remove and re-insert the battery. If the device does not have a removable battery, perform the following steps: 1. Restart the device in Recovery mode: a. Restart the device by pressing the Power and Volume down buttons. When the device restarts, quickly press and hold the Volume up, Home and Power buttons. b. When the device displays the Recovery mode screen, release the Volume up, Home and Power buttons. c. Wait for the Recovery menu to be displayed (this can take several minutes). 2. Select Power off, then press the Power button to turn off the device. Note: Use the Volume up and Volume down buttons to navigate the Recovery menu. CONSOLE 4. Follow the on-screen instructions to place the device in Download mode, then connect the required cable to the device and UFED. 5. Click Continue. The following window appears. Attention This method requires the device's firmware to be flashed. In some cases the device may experience unexpected behavior and you will need to flash the original device firmware, which causes a device wipe. Before using this method, we recommend trying other Physical bootloader methods. | CONTINUE 6. Click Continue to flash the device's firmware. The following window appears. Attention 1. Disconnect the device from the UFED. 2. Press on the power button until the device restarts. 3.Turn off the device. 4. Press and hold "Vol Down + PWR" + "Home" (or "Bixby") until the device displays boot menu. 5. Press Volume Up button. 6. Connect the cable to the device. 7. Connect the cable to the UFED. 8. Select Continue. CONTINUE


WAITING FOR DEVICE
Samsung CDMA SM-G930V Galaxy S7
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
SM-G930V Galaxy S7:
Note: This method is supported for devices running Android OS up to and including 7.1.1.
Android OS 8.0 and above is not supported and bootloop issues may occur.
To allow device connection:
Note: The device battery should be fully charged.
1. Turn off the device.
2. Press and hold the Volume down, Home and Power buttons until the device enters Download mode.
3. Select "Continue" by pressing the Volume up button.
4. Wait until the Download mode logo appears on the device screen, and then connect the device to the cable.
5. Connect the cable to UFED 4PC.
6. Select "Continue".
If a password is required to turn the device off, remove and re-insert the battery.
If the device does not have a removable battery, perform the following steps:
1. Restart the device in Recovery mode:
a. Restart the device by pressing the Power and Volume down buttons. When the device restarts, quickly press and hold the Volume up, Home and Power buttons.
b. When the device displays the Recovery mode screen, release the Volume up, Home and Power buttons.
c. Wait for the Recovery menu to be displayed (this can take several minutes).
2. Select Power off, then press the Power button to turn off the device.
Note: Use the Volume up and Volume down buttons to navigate the Recovery menu.
ABORT
BACK
CONSOLE
CONTINUE

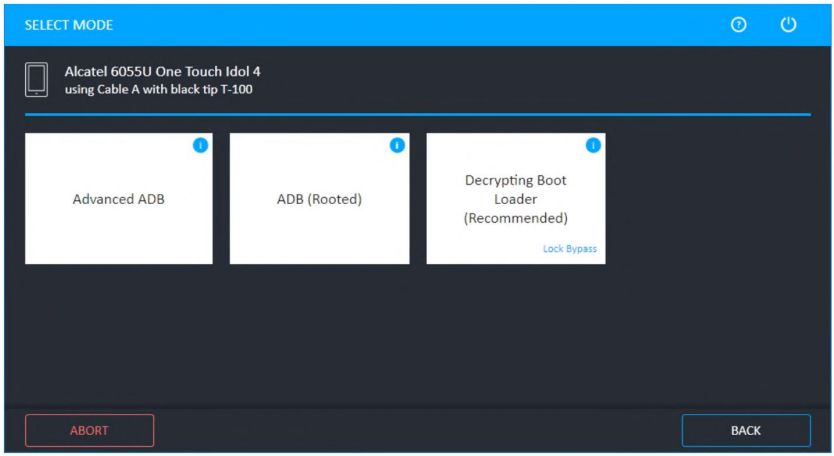

Attention
1. Disconnect the device from the UFED.
2. Press on the power button until the device restarts.
3.Turn off the device.
4. Press and hold "Vol Down + PWR" + "Home" (or "Bixby") until the device displays boot menu.
5. Press Volume Up button.
6. Connect the cable to the device.
7. Connect the cable to the UFED.
8. Select Continue.
CONTINUE

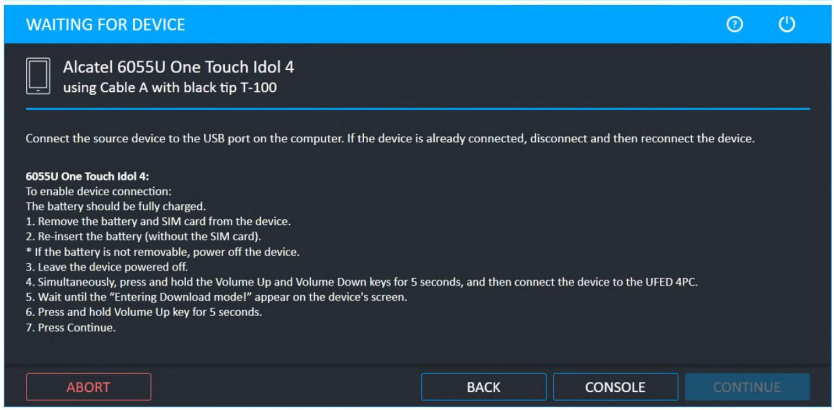
7. Follow the on-screen instructions to place the device in Download mode again, then connect the required cable to the device and UFED. 8. Click Continue. The following window appears. Attention During device exploitation, UFED will temporarily corrupt the device's recovery partition (leaving the user data partition untouched). Upon success, UFED will immediately restore the recovery partition to its previous state, and follow to produce the physical extraction. In the unexpected case of failure, the device may be left in a state where it can operate and boot normally into Android, but without the capability to boot into recovery mode until the recovery partition is re-flashed with any original (carrier) or alternative (e.g. TWRP) recovery image. In such cases where restoring recovery capability is required, the operator is instructed to obtain a matching recovery image and flash it using the standard Odin tool. Continue extraction? | CONTINUE 9. Click Continue. The Extraction in Progress window appears. EXTRACTION IN PROGRESS Samsung CDMA SM-G930V Galaxy S7 using Cable A with black tip T-100 Please wait, this can take some time... Connecting 10. Follow any on-screen instructions.


Attention
During device exploitation, UFED will temporarily corrupt the device's recovery partition (leaving the user data partition untouched). Upon success, UFED will immediately restore the recovery partition to its previous state, and follow to produce the physical extraction.
In the unexpected case of failure, the device may be left in a state where it can operate and boot normally into Android, but without the capability to boot into recovery mode until the recovery partition is re-flashed with any original (carrier) or alternative (e.g. TWRP) recovery image. In such cases where restoring recovery capability is required, the operator is instructed to obtain a matching recovery image and flash it using the standard Odin tool.
Continue extraction?
ABORT
CONTINUE

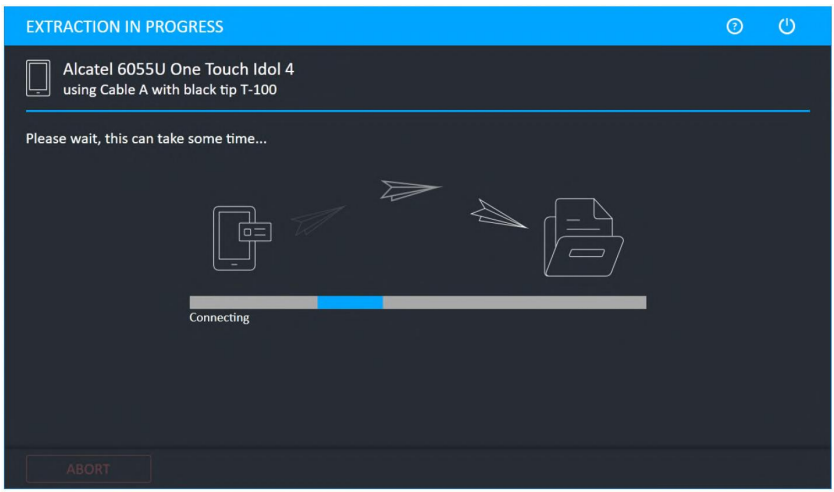

EXTRACTION IN PROGRESS
Samsung CDMA SM-G930V Galaxy S7
using Cable A with black tip T-100
Please wait, this can take some time...
Connecting
ABORT

6.5. Decrypting boot loader This extraction method performs a physical extraction on encrypted Android devices with the following Qualcomm chipsets: 8909, 8916, 8939, 8952, and 8396. It performs the extraction when the device Is in boot loader mode. It bypasses the user lock and is forensically sound. To perform a Decrypting boot loader extraction: 1. Click Mobile device and identify the device, then click Physical. The Select Mode window appears: SELECT MODE Alcatel 6055U One Touch Idol 4 using Cable A with black tip T-100 Decrypting Boot Advanced ADB ADB (Rooted) Loader (Recommended) 2. Click Decrypting Boot Loader. For information on using optional timeframe and party filters, refer to the Overview Guide. The Select Extraction Location window appears. 3. Select the extraction location. The Waiting for Device window appears. WAITING FOR DEVICE (J Alcatel 6055U One Touch Idol 4 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. 6055U One Touch Idol 4: To enable device connection: The battery should be fully charged. 1. Remove the battery and SIM card from the device. 2. Re-insert the battery (without the SIM card). * If the battery is not removable, power off the device. 3. Leave the device powered off. 4. Simultaneously, press and hold the Volume Up and Volume Down keys for 5 seconds, and then connect the device to the UFED 4PC. 5. Wait until the “Entering Download mode!” appear on the device's screen. 6. Press and hold Volume Up key for 5 seconds. 7. Press Continue. CONSOLE Chapter 6: 85 en


SELECT MODE
Alcatel 6055U One Touch Idol 4
using Cable A with black tip T-100
Advanced ADB
ADB (Rooted)
Decrypting Boot Loader (Recommended)
Lock Bypass
ABORT
BACK


WAITING FOR DEVICE
Alcatel 6055U One Touch Idol 4
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
6055U One Touch Idol 4:
To enable device connection:
The battery should be fully charged.
1. Remove the battery and SIM card from the device.
2. Re-insert the battery (without the SIM card).
* If the battery is not removable, power off the device.
3. Leave the device powered off.
4. Simultaneously, press and hold the Volume Up and Volume Down keys for 5 seconds, and then connect the device to the UFED 4PC.
5. Wait until the "Entering Download mode!" appear on the device's screen.
6. Press and hold Volume Up key for 5 seconds.
7. Press Continue.
ABORT
BACK
CONSOLE
CONTINUE

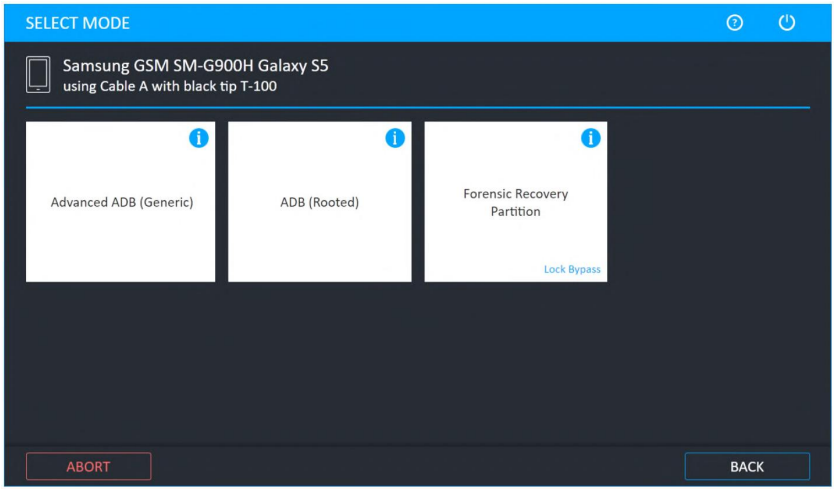
4. Follow the on-screen instructions to place the device in the required mode. Click Continue when enabled. Attention Disconnect the device from UFED, enter the specified mode (for example, key combination, EDL cable etc.) again using the previous instructions, and then press “Continue”. 5. Disconnect the device from UFED, enter the specified mode again [for example, key combination, EDL cable etc.} using the previous instructions, and then click Continue. The following window appears. EXTRACTION IN PROGRESS (J Alcatel 6055U One Touch Idol 4 using Cable A with black tip T-100 Please wait, this can take some time... LS Connecting 86


EXTRACTION IN PROGRESS
Alcatel 6055U One Touch Idol 4
using Cable A with black tip T-100
Please wait, this can take some time...
Connecting
ABORT

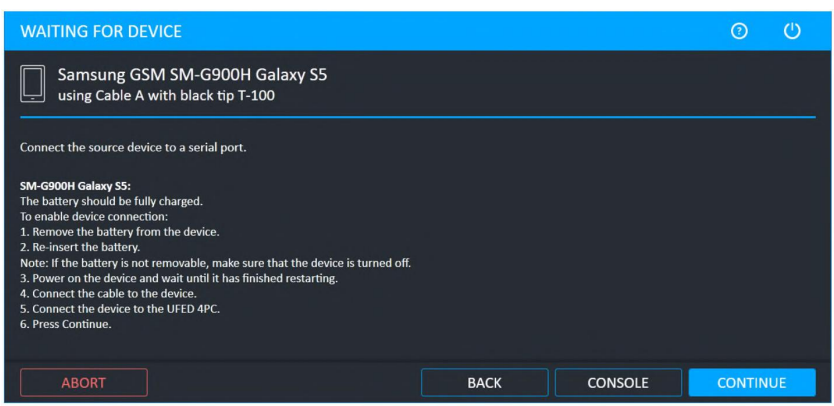
6.6. Forensic recovery partition An extraction method that performs a physical extraction while the device Is in recovery mode. UFED replaces the device's original recovery partition with Cellebrite’s custom forensic recovery partition. The original recovery partition on the Android device can be considered as an alternative boot partition that may also change the user data, while Cellebrite’s recovery partition does not affect any of the user data. This extraction method bypasses the user lock from a number of Samsung Android devices and is forensically sound. It does not support extractions from a memory or SIM card. For a complete list of supported devices, refer to the UFED Phone Detective Mobile App or the UFED Supported Devices document in MyCellebrite. It is recommended to use the Forensic recovery partition method when other physical extraction msm-ethods [e.g., Bootloader] are not successful, or not available [e.g., if the Android firmware version is not supported). If the device does not start correctly after using this extraction method, use the Exit Android Recovery Mode device tool. See Exit Android recovery mode [on page 127). To perform a forensic recovery partition extraction: 1. Click Mobile device and identify the device, then click Physical. The Select Mode screen appears: SELECT MODE (J Samsung GSM SM-G9O0H Galaxy S5 using Cable A with black tip T-100 Forensic Recovery Advanced ADB (Generic) ADB (Rooted) partition Chapter 6: 87 SE en nn

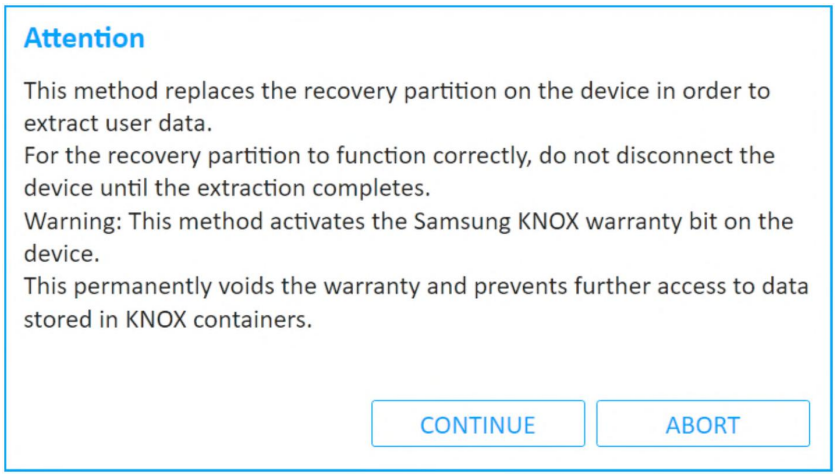
It is recommended to use the Forensic recovery partition method when other physical extraction msm-ethods (e.g., Bootloader) are not successful, or not available (e.g., if the Android firmware version is not supported).

If the device does not start correctly after using this extraction method, use the Exit Android Recovery Mode device tool. See Exit Android recovery mode (on page 127).

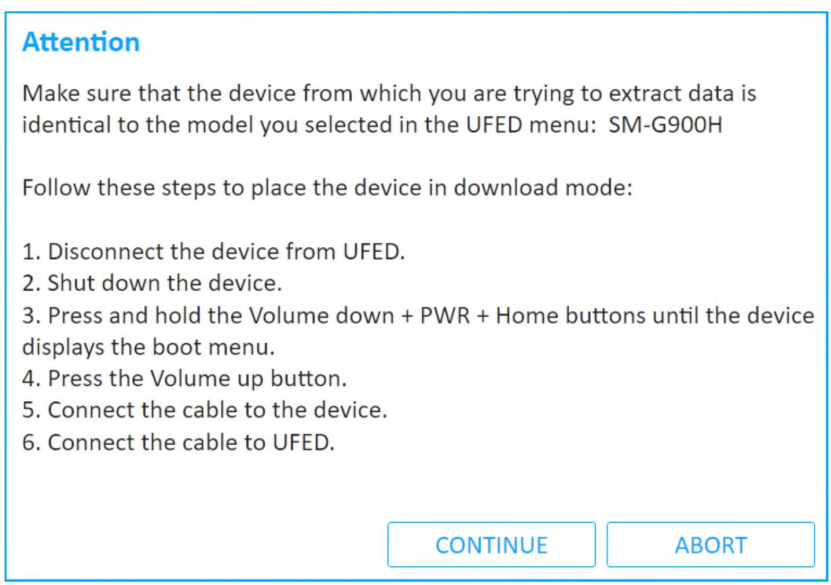

SELECT MODE
Samsung GSM SM-G900H Galaxy S5
using Cable A with black tip T-100
Advanced ADB (Generic)
ADB (Rooted)
Forensic Recovery Partition
Lock Bypass
ABORT
BACK

2. Select Forensic Recovery Partition. yp For information on using optional timeframe and party filters, refer to the Overview Guide. The following screen appears. The Waiting for Device screen appears. WAITING FOR DEVICE LJ Samsung GSM SM-GSO0H Galaxy S5 using Cable A with black tip T-100 Connect the source device to a serial port. SM-G900H Galaxy S5: The battery should be fully charged. To enable device connection: 1. Remove the battery from the device. 2. Re-insert the battery. Note: If the battery is not removable, make sure that the device is turned off. 3. Power on the device and wait until it has finished restarting. 4. Connect the cable to the device. 5. Connect the device to the UFED 4PC. 6. Press Continue. CONSOLE CONTINUE 3. Click Continue. The following warning is displayed. Attention This method replaces the recovery partition on the device in order to extract user data. For the recovery partition to function correctly, do not disconnect the device until the extraction completes. Warning: This method activates the Samsung KNOX warranty bit on the device. This permanently voids the warranty and prevents further access to data stored in KNOX containers. CONTINUE ABORT 88

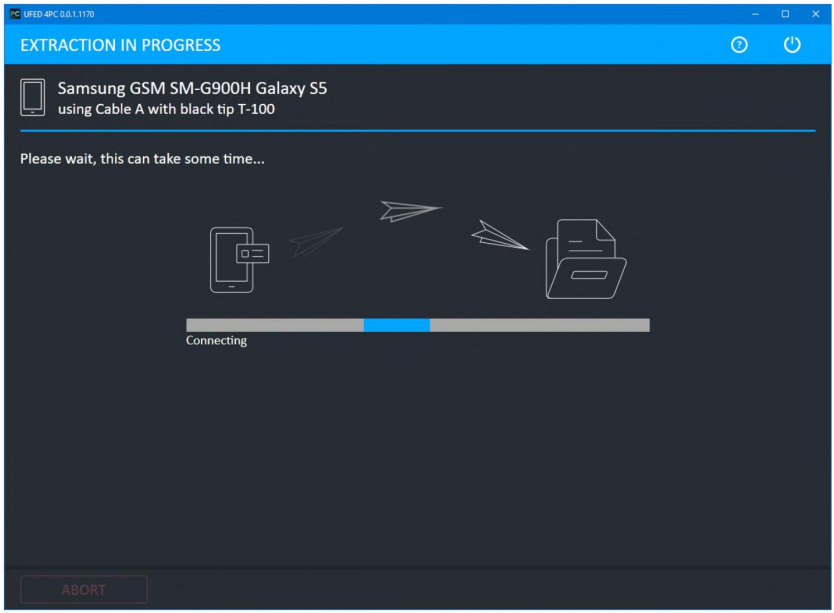

WAITING FOR DEVICE
Samsung GSM SM-G900H Galaxy S5
using Cable A with black tip T-100
Connect the source device to a serial port.
SM-G900H Galaxy S5:
The battery should be fully charged.
To enable device connection:
1. Remove the battery from the device.
2. Re-insert the battery.
Note: If the battery is not removable, make sure that the device is turned off.
3. Power on the device and wait until it has finished restarting.
4. Connect the cable to the device.
5. Connect the device to the UFED 4PC.
6. Press Continue.
ABORT
BACK
CONSOLE
CONTINUE


Attention
This method replaces the recovery partition on the device in order to extract user data.
For the recovery partition to function correctly, do not disconnect the device until the extraction completes.
Warning: This method activates the Samsung KNOX warranty bit on the device.
This permanently voids the warranty and prevents further access to data stored in KNOX containers.
CONTINUE
ABORT

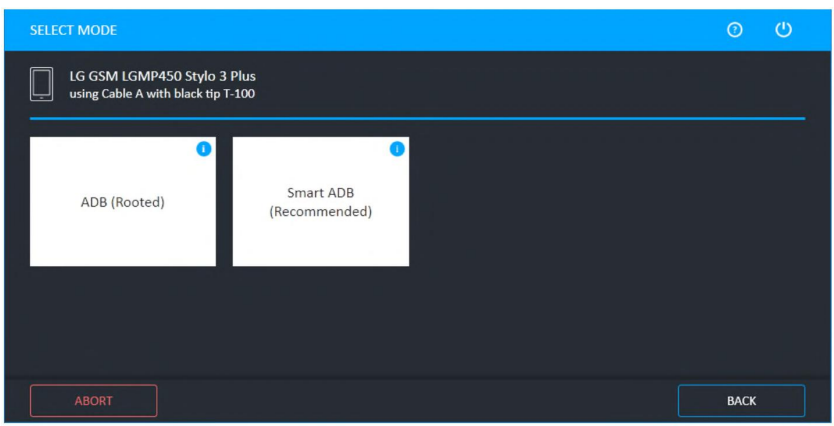
4. Click Continue. The device will be placed in download mode. The following screen appears. Attention Make sure that the device from which you are trying to extract data is identical to the model you selected in the UFED menu: SM-G900H Follow these steps to place the device in download mode: 1. Disconnect the device from UFED. 2. Shut down the device. 3. Press and hold the Volume down + PWR + Home buttons until the device displays the boot menu. 4. Press the Volume up button. 5. Connect the cable to the device. 6. Connect the cable to UFED. CONTINUE ABORT 5. Click Continue. The following screen appears. Attention Confirm the connected model is SM-G9OOH. While the device is in download mode, the model name will be printed on CONTINUE ABORT 6. Click Continue. The following screen appears. the device's screen. 7. Follow the instructions to place the device in Download mode. Force it to restart by pressing the Power and Volume down buttons. When the device restarts, quickly press the Volume up, Home and Power buttons. Click Continue when Downloading appears on the device's screen (this can take a few minutes]. Chapter 6: 89


Attention
Make sure that the device from which you are trying to extract data is identical to the model you selected in the UFED menu: SM-G900H
Follow these steps to place the device in download mode:
1. Disconnect the device from UFED.
2. Shut down the device.
3. Press and hold the Volume down + PWR + Home buttons until the device displays the boot menu.
4. Press the Volume up button.
5. Connect the cable to the device.
6. Connect the cable to UFED.
CONTINUE
ABORT

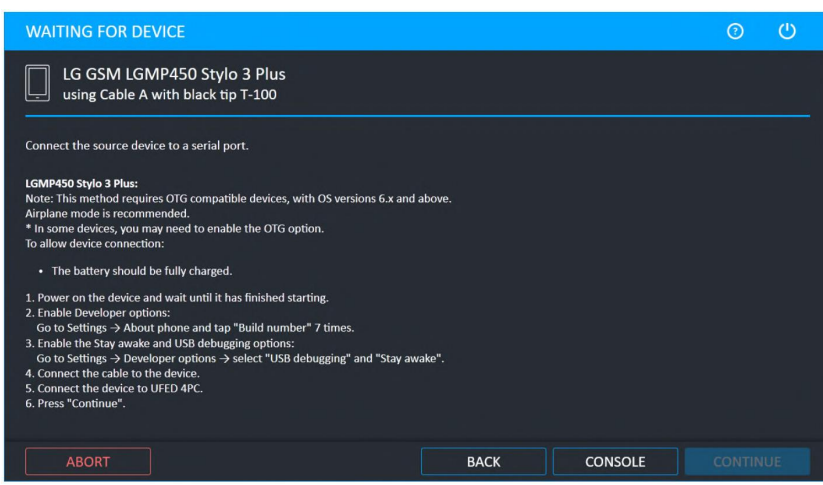
The Extraction in Progress screen appears. UFED 4PC 0.0.1.1170 EXTRACTION IN PROGRESS LJ Samsung GSM SM-GS900H Galaxy S5 using Cable A with black tip T-100 Please wait, this can take some time... Ei Connecting 8. Follow any on-screen instructions. 90



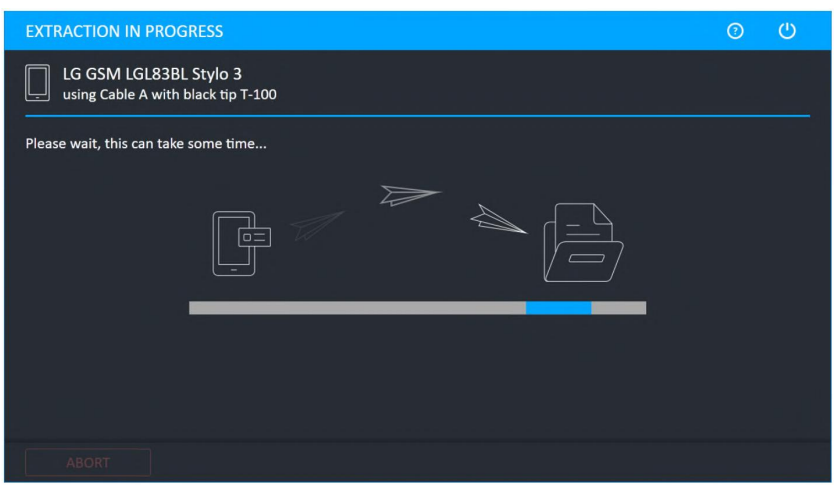
6.7. Smart ADB The Smart ADB extraction method enables you to perform physical extractions on Android devices that include the “November 2016" security patch. This method is supported by OTG compatible devices, with OS versions 6.0 and above. Only security unlocked devices are Supported. On some devices, you may need to enable the OTG option. It is recommended to place the device in Flight mode. If a specific device is not supported, we recommend that you use a similar model or any generic Advanced ADB profile. To perform a Smart ADB extraction: 1. Click Mobile device and identify the device, then click Physical. The Select Mode screen appears: SELECT MODE [| LG GSM LGMP450 Stylo 3 Plus L) using Cable A with black tip T-100 Smart ADB ed (Recommended) 2. Click Smart ADB. For information on using optional timeframe and party filters, refer to the Overview Guide. The Waiting for Device screen appears. Chapter 6: 71 nn nnn



WAITING FOR DEVICE (] LG GSM LGMP450 Stylo 3 Plus using Cable A with black tip T-100 Connect the source device to a serial port. LGMP450 Stylo 3 Plus: Note: This method requires OTG compatible devices, with OS versions 6.x and above. Airplane mode is recommended. * In some devices, you may need to enable the OTG option. To allow device connection: * The battery should be fully charged. 1. Power on the device and wait until it has finished starting. 2. Enable Developer options: Go to Settings > About phone and tap “Build number" 7 times. 3. Enable the Stay awake and USB debugging options: Go to Settings > Developer options > select "USB debugging" and "Stay awake". 4. Connect the cable to the device. 5. Connect the device to UFED 4PC. 6. Press "Continue". CONSOLE 3. Follow the on-screen instructions then click Continue. The following window appears. Attention UFED will now try to flash another image to the device. Press and hold the Volume down, Power and Home (or Bixby) buttons, until the device displays the Warning screen. Then press Volume up and select "Continue" in UFED. CONTINUE 4. Click Continue. The following window appears. Process complete Disconnect the device and connect Cable No. 500 (side A) to UFED. Note: If required, this process flashes new firmware to the cable. You can also use “Tools” > “Flash Cable 500 Firmware”. ABORT CONTINUE 5. Disconnect the device and connect Cable No. 500 (side A) to UFED, then click Continue. The initializing stage can take up to 30 minutes. 92


WAITING FOR DEVICE
LG GSM LGMP450 Stylo 3 Plus
using Cable A with black tip T-100
Connect the source device to a serial port.
LGMP450 Stylo 3 Plus:
Note: This method requires OTG compatible devices, with OS versions 6.x and above.
Airplane mode is recommended.
* In some devices, you may need to enable the OTG option.
To allow device connection:
• The battery should be fully charged.
1. Power on the device and wait until it has finished starting.
2. Enable Developer options:
Go to Settings → About phone and tap "Build number" 7 times.
3. Enable the Stay awake and USB debugging options:
Go to Settings → Developer options → select "USB debugging" and "Stay awake".
4. Connect the cable to the device.
5. Connect the device to UFED 4PC.
6. Press "Continue".
ABORT
BACK
CONSOLE
CONTINUE

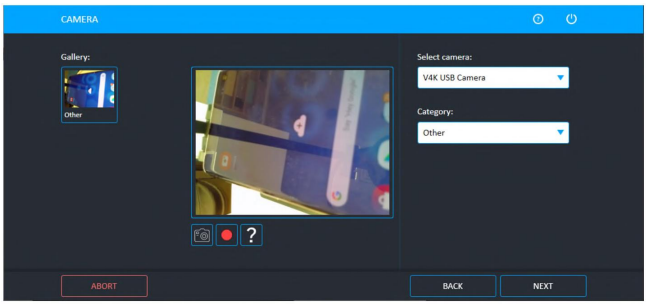
If required, this process flashes new firmware to the cable. You can also use the Flash Cable 500 Firmware [on page 127) tool. The following window appears. Process complete Connect Cable No. 501 to the device and the other end of the cable to Cable No. 500. CONTINUE 6. Connect Cable No. 501 {or other specified cable) to the device and the other end of the cable to Cable No. 500, then click Continue. The initialization process starts. The following window appears. Attention Disconnect the cables, and connect the device to UFED with Cable No. 100. CONTINUE 7. Disconnect Cable No. 500 and reconnect the device using Cable No. 100 [or other specified cable]. Click Continue to start the extraction. The following window appears. EXTRACTION IN PROGRESS LG GSM LGL83BL Stylo 3 using Cable A with black tip T-100 Please wait, this can take some time... C When the extraction completes, the Extraction completed successfully window appears. If Cellebrite UFED/Responder could not find a setting for the specific device, UFED can Chapter 6: 6:



attempt other potential settings. This process requires user interaction and takes time to complete. 8. Click Continue to try the extraction with other settings. The following window appears. Attention Completed attempt 1/3 with setting number 1. Retrying with current setting. Disconnect the cables, and connect the device to UFED with Cable No. 100. ABORT RETRY 9. Disconnect the cables and connect the device to UFED with Cable No. 100 (or specified cable}, then click Retry. 94

7. Capture images and screenshots The Cellebrite UFED camera enables you to collect evidence by taking pictures or videos of a device (see Capturing images [on the next page]. You can also use a Screenshot feature to capture internal screenshots directly from a Blackberry, Android or iOS device [see Capturing screenshots (on page 100)). Both these options can be useful as complimentary evidence or in instances when data cannot be extracted from a device. You can add notes, categories and bookmarks to the pictures and videos, which will be visible in Physical/Logical Analyzer. The collected evidence can be shown within a standalone custom report or in addition to the extracted information. The report includes information about the device, connection type, Cellebrite UFED version, and serial number. Image information includes file name link, file size, date and time, MD5 and SHA256 hash information. The images are located in a folder called Snapshots and are in PNG format. Video information includes file name, file size, date and time, and a link to the file. The videos are located ina folder called Videos and are in AVI format. 7.1. The Cellebrite UFED camera The Cellebrite UFED camera Is offered as an add-on and It is controlled by the Cellebrite UFED/Responder. All necessary drivers are preinstalled with the application. The Cellebrite UFED camera includes a camera stand, which enables you to adjust the height and the angle of the Cellebrite UFED camera, a pad to place the device, and an anti-glare pad to prevent glare when taking pictures. Connect the camera to an available USB port of the computer. Chapter 7: 9D

7.2. Capturing images You can take pictures or videos of a device. To capture images or videos: 1. Click Camera. The Select Extraction Location screen appears. 2. Connect the Cellebrite UFED camera to a USB port on the computer. The following window appears. CAMERA Gallery: Select camera: V4K USB C. Category: ® If you have multiple cameras, you can choose the required camera in Select camera box. 96



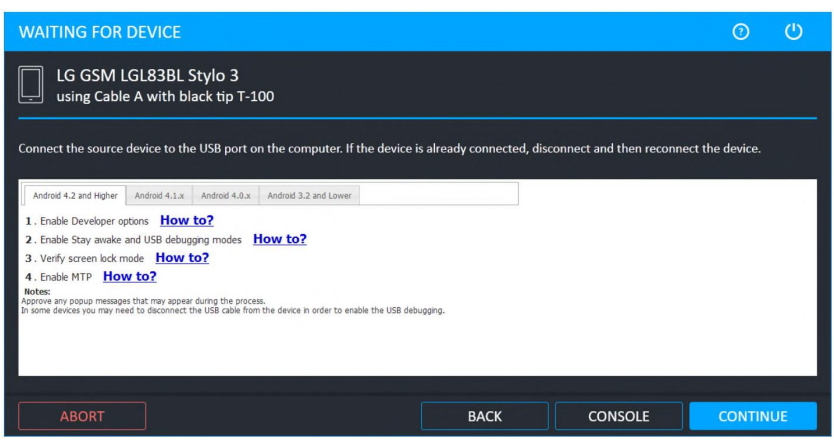
If you have multiple cameras, you can choose the required camera in Select camera box.

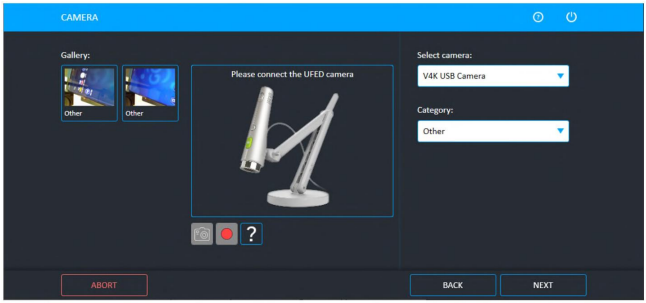
3. Do one of the following: » Click fe | to start a video recording and click ee. stop the video recording. » Click to take a picture. » Click Other to change the default category. Images and videos will be displayed In Physical/Logical under these categories. » Click an image or video, to add notes, bookmarks (a). categories (C3), or delete the file (i). Click [5) to move back to live view. To rotate a picture or video, or play a recorded video, click the picture or video, and then click the picture or video in the leftmost screen. Use the rotate buttons or video buttons 44 Pip roc . See the following examples. Chapter 7: 7)

18558
17:31
S Travel
Get your news and social updates all in one place
Contacts
Internet
Phone
Apps

00:0002/000016 4 qj - rrProc ¢ 4. Click Next to continue.
Chapter 7: ss Oe

7.3. Capturing screenshots The Screenshot feature captures internal screenshots directly from a Blackberry, Android or iOS device. To capture screenshots from the devices: 1. Click Mobile device and identify the device, then click Screenshots. The Select Extraction Location screen appears. The Waiting for Device screen appears. WAITING FOR DEVICE (J LG GSM LGL83BL Stylo 3 using Cable A with black tip T-100 Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. Android 4.2 and Higher | Android 4.1.x Android 4.0.x Android 3.2 and Lower . Enable Developer options How to? . Enable Stay awake and USB debugging modes How to? . Verify screen lock mode How to? . Enable MTP How to? tes: Approve any popup messages that may appear during the process. In some devices you may need to disconnect the USB cable from the device in order to enable the USB debugging. CONSOLE CONTINUE 2. Follow the instructions to connect the device. 3. Click Continue. The Screenshots screen appears. CAMERA Gallery: Select camera: , Please connect the UFED camera V4K USB Camera Y Category: If you have multiple cameras, you can choose the required camera in Select camera box. 100

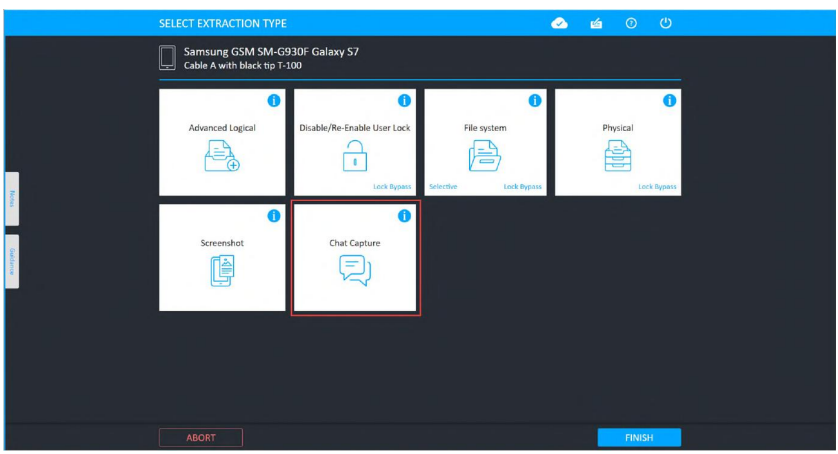

WAITING FOR DEVICE
LG GSM LGL83BL Stylo 3
using Cable A with black tip T-100
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
Android 4.2 and Higher
Android 4.1.x
Android 4.0.x
Android 3.2 and Lower
1. Enable Developer options How to?
2. Enable Stay awake and USB debugging modes How to?
3. Verify screen lock mode How to?
4. Enable MTP How to?
Notes:
Approve any popup messages that may appear during the process.
In some devices you may need to disconnect the USB cable from the device in order to enable the USB debugging.
ABORT
BACK
CONSOLE
CONTINUE



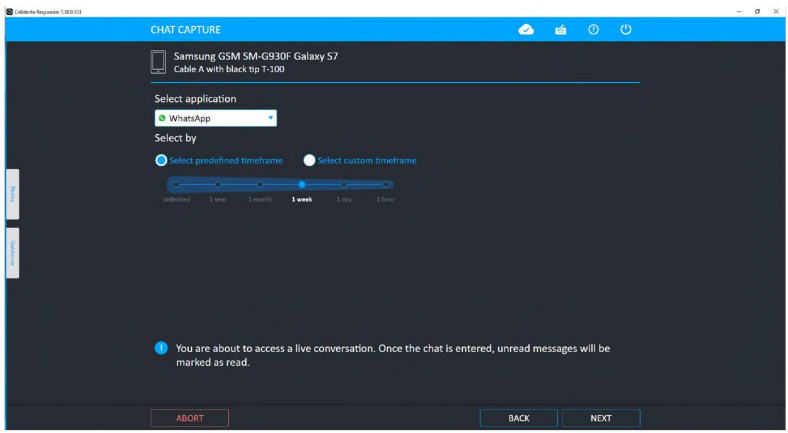
If you have multiple cameras, you can choose the required camera in Select camera box.

4. Capture the desired screenshots and click Next. The Capture Screenshots Summary screen appears. Chapter 7: 101 Oe

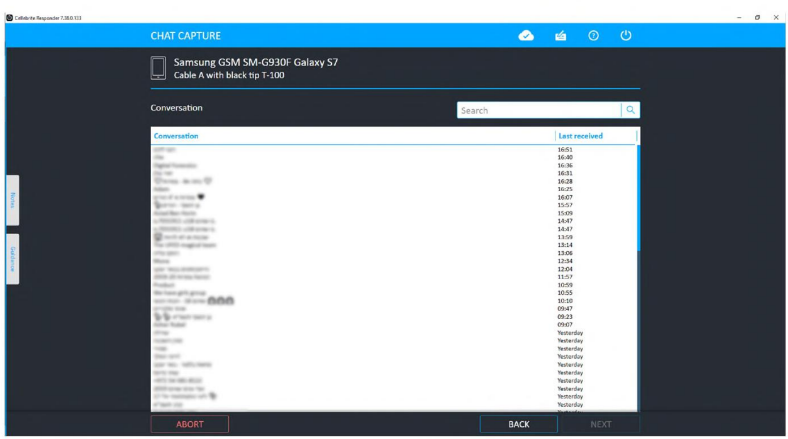
8. Chat capture Chat Capture is an automated screen capturing process that allows users to extract and analyze selective chat conversations from third party application data. There are two modes available: » By application - Automatically capture data from supported apps like WhatsApp based on conversation name and date range. Users can also perform text search on the captured screens. » Generic - Semi-automated mode to capture any scrollable area on the device screen. 8.1. Performing a Chat capture by application In addition to capturing the chat, this mode will also capture chat information such as chat name and participant details. 1. Click Mobile device and identify the device, then click Chat capture. |B ceterite Responder? 38012 SELECT EXTRACTION TYPE ia Samsung GSM SM-G930F Galaxy S7 (=) Cable A with black tip T-100 Chat Capture 2) FINISH 2. Select the application from which to capture a chat. 3. Select a predefined timeframe or create a custom timeframe. 4. Click Next. When using Chat capture, you are entering a live conversation. Once a chat Is entered, unread messages will be marked as read. 102



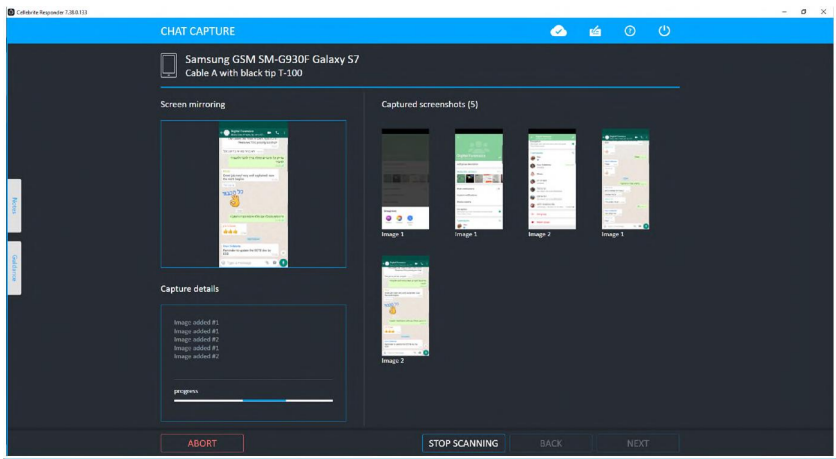
CHAT CAPTURE ia Samsung GSM SM-G930F Galaxy S7 Cable A with black tip T-100 Select application © WhatsApp MY Select by co) You are about to access a live conversation. Once the chat is entered, unread messages will be marked as read. CHAT CAPTURE ial Samsung GSM SM-G930F Galaxy S7 (=) Cable A with black tip T-100 Conversation 6. Click Next. 7. The chat will be automatically captured. The captured screens appear under Captured screenshots. Click Stop scanning if you wish to stop the scanning process. Chapter 8: 103

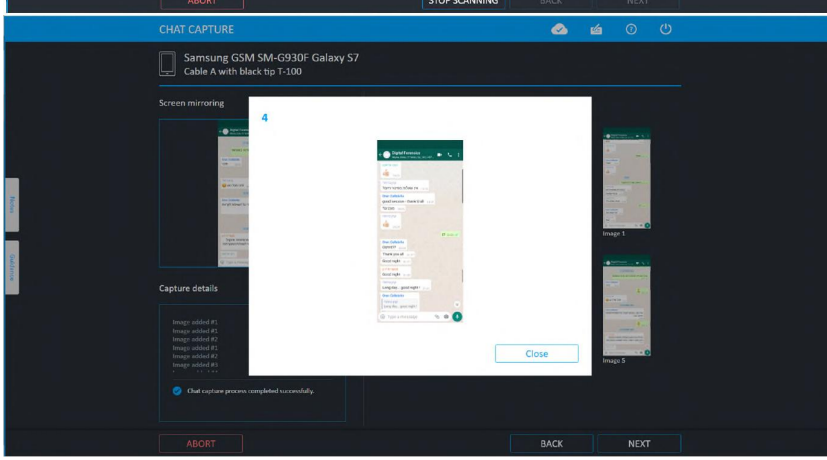


5. Select a chat from the list or use the search bar to find a chat.

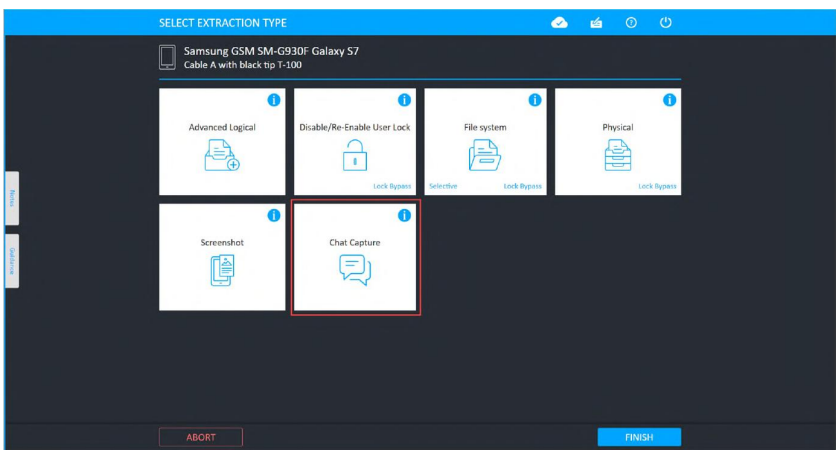


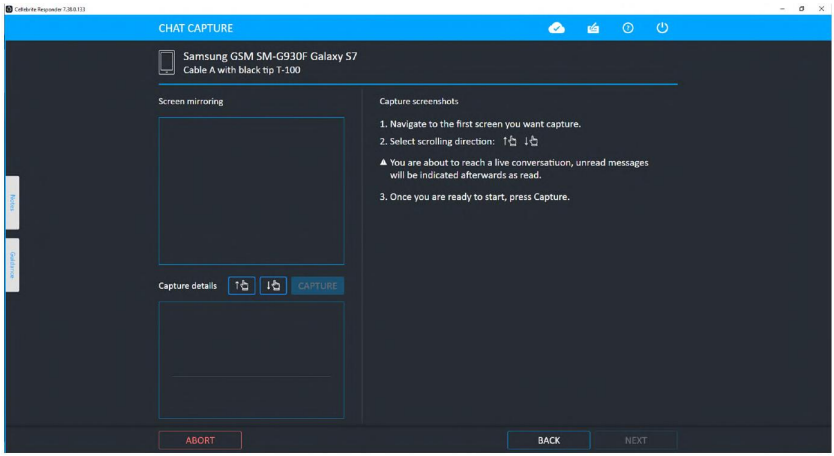
CHAT CAPTURE O Samsung GSM SM-G930F Galaxy S7 (=) Cable A with black tip T-100 Captured screenshots (5) la —s = Image 1 Image 1 Image 2 Image 1 — STOP SCANNING 8. To viewa single screentshot, click on it to enlarge. | ceterie Responder? 3801 9. Click Next when finished. Captured screenshots can be viewed and analyzed in Physical/Logical Analyzer under the Chats model. 8.2. Performing a Chat capture in Generic mode In addition to capturing chats, Generic mode can be useful to capture any element of data such as social media feeds, forums, etc. 104



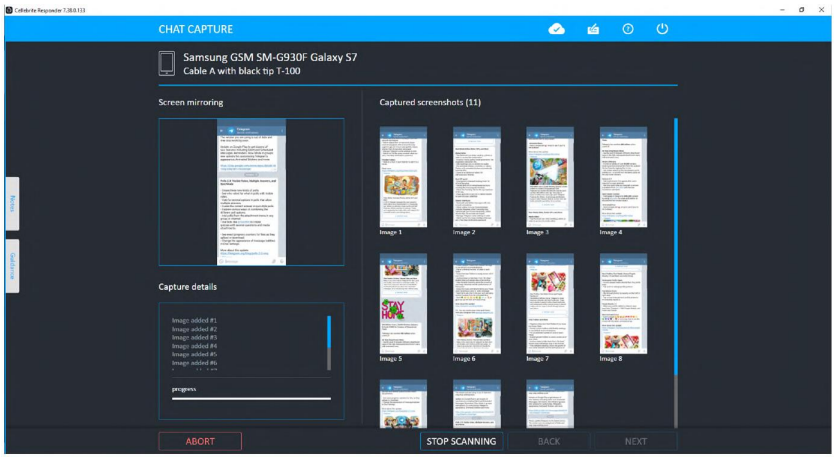


1. Click Mobile device and identify the device, then click Chat capture. [BD ceterte Responder 73801, Sig. SELECT EXTRACTION TYPE Oo Samsung GSM SM-G930F Galaxy S7 =} Cable A with black tip T-100 Advanced Logical Disable/Re-Enable User Lock Physical fe en Screenshot Chat Capture e | & Select Generic. Click Next. Navigate to the relevant app and then to the first screen that you want to capture. t | 9. Select scrolling direction (re) (08) 6. When ready, click Capture. CHAT CAPTURE ial Samsung GSM SM-G930F Galaxy S7 (=) Cable A with black tip T-100 Screen mirroring Capture screenshots 1. Navigate to the first screen you want capture. 2. Select scrolling direction: 19 1% 4 You are about to reach a live conversatiuon, unread messages will be indicated afterwards as read. 3. Once you are ready to start, press Capture. Capture details 7. The chat will be automatically captured. The captured screens appear under Captured screenshots. Chapter 8: 105 Oe




Cellebrite Responder 7.38.0.133
CHAT CAPTURE
Samsung GSM SM-G930F Galaxy S7
Cable A with black tip T-100
Screen mirroring
Capture screenshots
1. Navigate to the first screen you want capture.
2. Select scrolling direction:
▲ You are about to reach a live conversatiuon, unread messages will be indicated afterwards as read.
3. Once you are ready to start, press Capture.
Capture details
CAPTURE
ABORT
BACK
NEXT

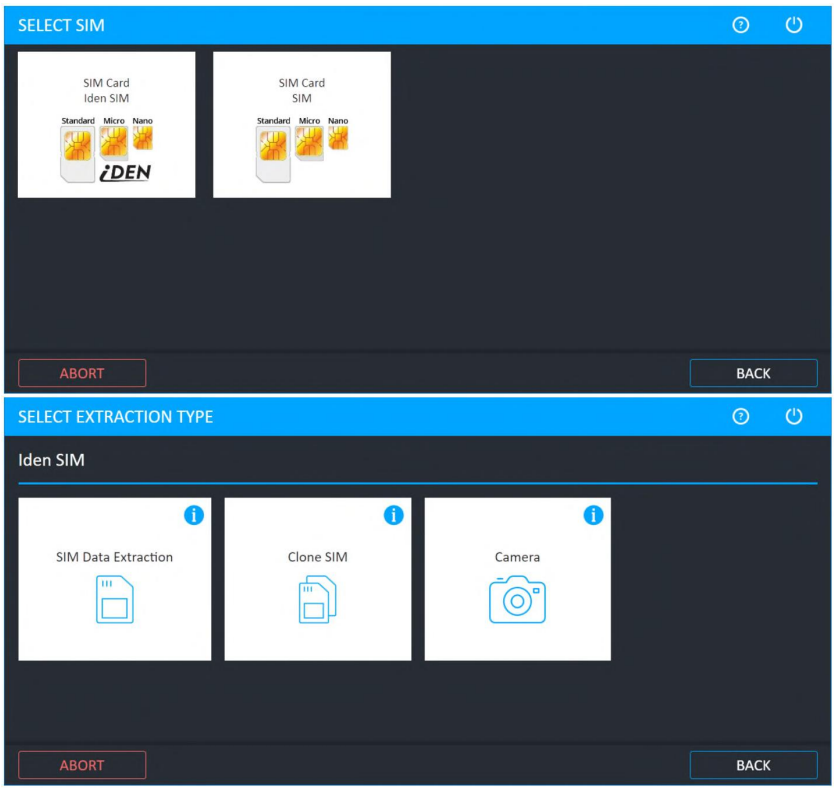
CHAT CAPTURE ia Samsung GSM SM-G930F Galaxy S7 (=) Cable A with black tip T-100 Captured screenshots (11) wa “= _— = st Image S Image 6 Image 7 Image 8 STOP SCANNING 8. To viewa single screentshot, click on it to enlarge. 9. Click Next when finished. Captured screenshots in Generic mode can be viewed and analyzed in Physical/Logical Analyzer or Responder viewer under the Images model. You will be able to perform a text search of the captured screens but only in chat applications that support the search functionality. *Available in Physical/Logical Analyzer only. 106



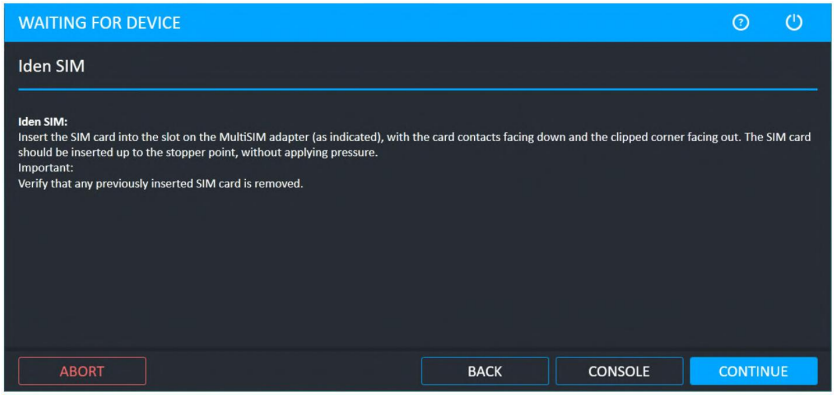
Captured screenshots in Generic mode can be viewed and analyzed in Physical/Logical Analyzer or Responder viewer under the Images model.

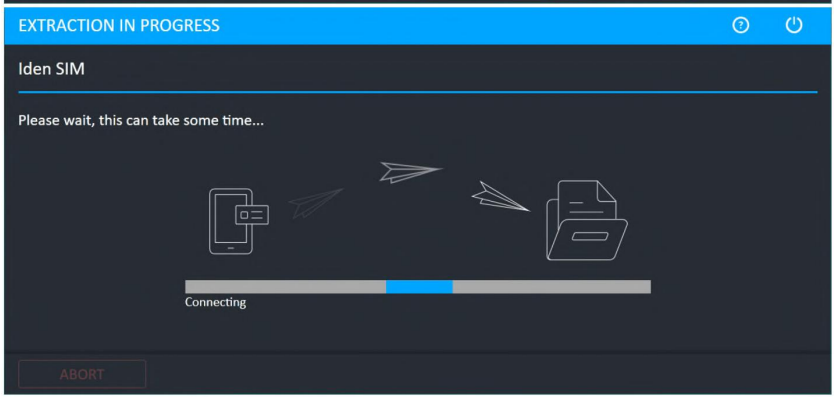
You will be able to perform a text search of the captured screens but only in chat applications that support the search functionality. *Available in Physical/Logical Analyzer only.

9. SIM card functionality The SIM Card functions enable you to perform various SIM card related functions: >» Sim data extraction >» Clone SIM » File system extraction 9.1. SIM data extraction The SIM Data Extraction function enables you to perform logical extraction from a SIM or USIM card. 9.1.1. Performing SIM data extraction The following example is performed using a SIM Card. To perform the SIM Data Extraction: 1. Click SIM Card. The following window appears. SELECT SIM SIM Card SIM Card Iden SIM SIM Standard Micro Nano Standard Micro Nano cDEN 2. Click either SIM or Iden SIM. The Select Extraction Type window appears. SELECT EXTRACTION TYPE Iden SIM Camera Chapter 9: 107

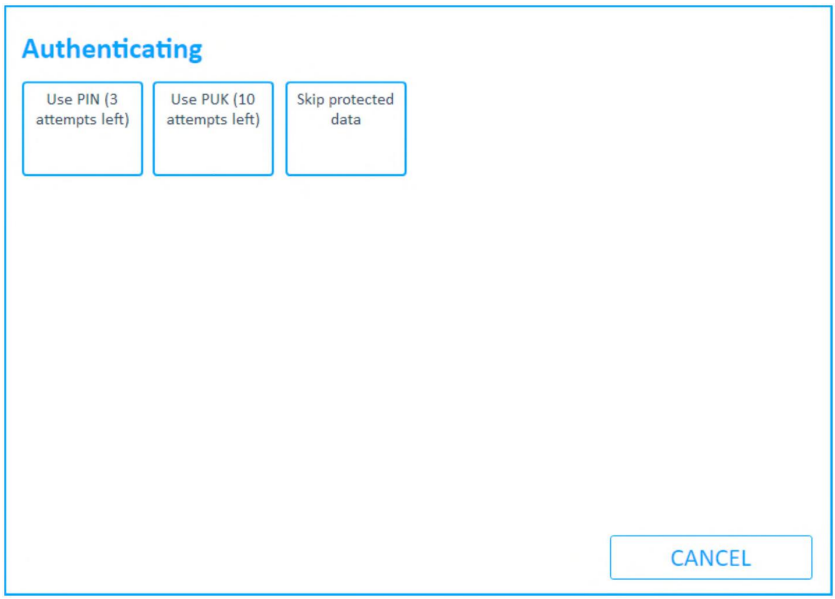


3: Click SIM Data Extraction. The Select Extraction Location window appears. The Waiting for Device screen appears. WAITING FOR DEVICE Iden SIM Iden SIM: Insert the SIM card into the slot on the MultiSIM adapter (as indicated), with the card contacts facing down and the clipped corner facing out. The SIM card should be inserted up to the stopper point, without applying pressure. Important: Verify that any previously inserted SIM card is removed. CONSOLE CONTINUE Insert the SIM card into the SIM card slot. Click Continue. The extraction begins. EXTRACTION IN PROGRESS Iden SIM Please wait, this can take some time... Connecting The following window appears. 108


WAITING FOR DEVICE
Iden SIM
Iden SIM:
Insert the SIM card into the slot on the MultiSIM adapter (as indicated), with the card contacts facing down and the clipped corner facing out. The SIM card should be inserted up to the stopper point, without applying pressure.
Important:
Verify that any previously inserted SIM card is removed.
ABORT
BACK
CONSOLE
CONTINUE



Authenticating Use PIN (3 Use PUK (10 Skip protected attempts left) attempts left) data CANCEL Chapter 9: 109 ee

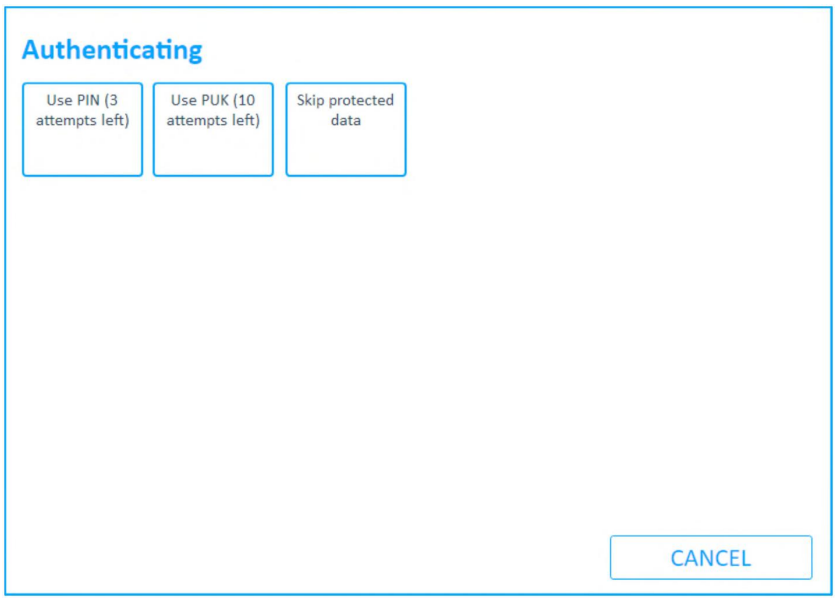


6. Click Use PIN, Use PUK or tap Skip protected data.

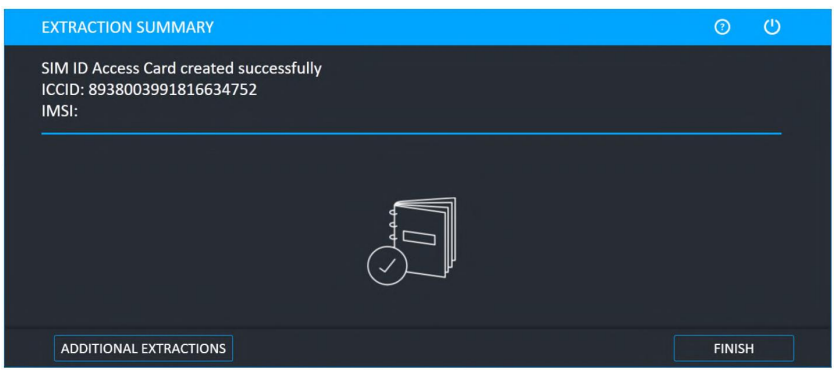
9.1.1.1. The extracted SIM data folder At the end of the SIM data extraction process, the extracted SIM data Is saved in the location you selected previously. The extracted SIM data folder is named “UFED SIM card” with the extraction date and counter: “UFED SIM card SIM card <DATE> (001)" If you selected to extract to the local drive, the extracted SIM data folder is located inside the application's Backup folder. The extracted SIM data folder contains a forensic report of extracted data in both HTML and XML formats and call log file (*.clog). 110

9.2. Clone SIM The Clone SIM ID function enables you to copy the SIM ID from one SIM card to a UFED SIM ID Access Card. Cloning the SIM ID provides a suitable solution to several problems facing forensic examiners, by allowing extraction of the device data: » While preventing the cellular device from connecting to the network, rendering the device invisible to the network without the ability to send or receive calls or SMS messages, and thereby preserving the device's current information. [No Faraday Bag is required to block RF signals). » When the original SIM ts not available, by manually programming the ICCID or IMSI into the Cloned SIM ID Card to mimic the original missing card. »» When the SIM card is PIN locked, by cloning the identification of the original SIM, which allows extraction of the device data without losing critical data including call history and SMS messages. There are three different ways that a SIM card can be cloned: » Clone an existing SIM card - to create a cloned SIM to use to extract device data without a network connection. See Cloning an existing SIM card ID [belowl. » Manually enter SIM data - to manually program the ICCID and IMSI to the cloned SIM card. See Entering SIM data manually (on page 114). » Create GSM Test SIM - The GSM test SIM card is used to extract device data when the original SIM is not available - a default ICCID and IMSI are programmed into the Cloned SIM ID Card to mimic the original missing card. See Creating a GSM test SIM [on page 118). 9.2.1. Cloning an existing SIM card ID Chapter 9: 111

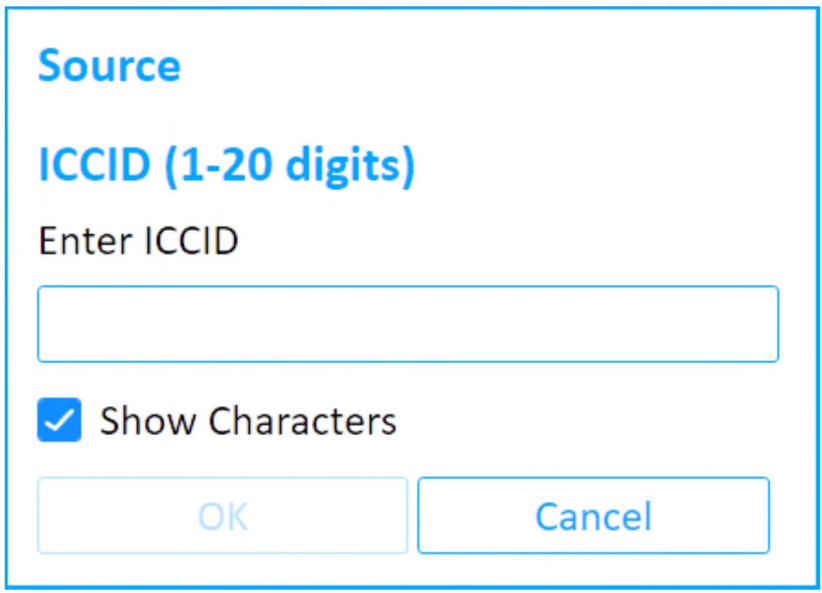
To select the source and clone the SIM card: The Select Source screen appears. Select Source Clone an Manually enter Create GSM existing SIM SIM data Test SIM card 4. Click Clone an existing SIM card. The Clone SIM ID prompt appears. Clone SIM ID Insert Source SIM into the UFED Device Adapter with the SIM card's contacts facing down and the clipped corner pointing toward you. CONTINUE 5. Check that the right SIM was inserted into the SIM card reader slot. 6. Click Continue. The following window appears. Authenticating Use PIN (3 Use PUK (10 Skip protected attempts left) attempts left) data CANCEL Ne



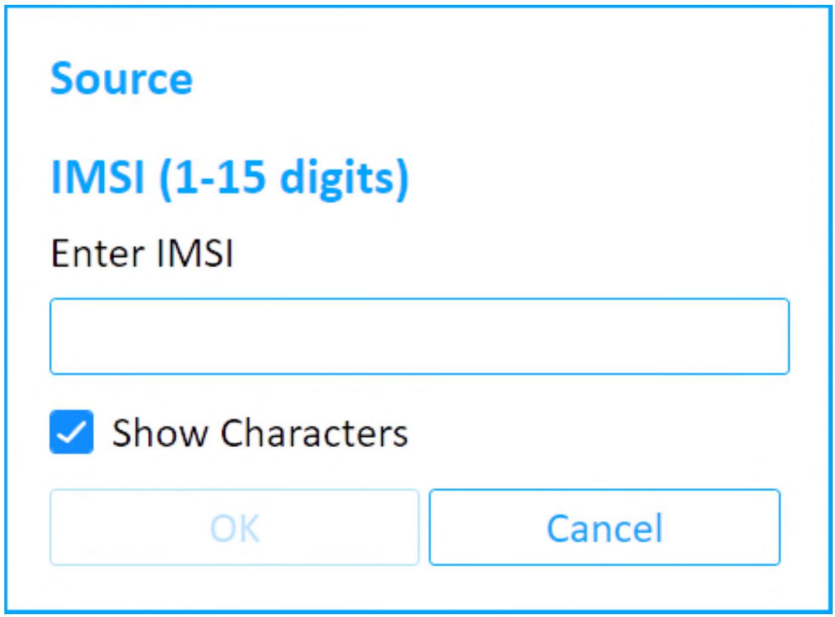
7. Click Use PIN, Use PUK or tap Skip protected data. The Extraction in Progress Source screen appears. When the information has been extracted from the SIM, the Insert Target Card prompt appears. Insert Target Card Insert SIM ID Access Card into the UFED Device Adapter with the SIM card's contacts facing down and the clipped corner pointing toward you. CONTINUE Remove the original SIM card from the SIM card reader. Insert a UFED SIM ID Access Card into the SIM slot. 10. Click Continue. At the end of the data process, a summary of the SIM cloning process Is displayed, detailing the ICCID and IMSI information of the cloned SIM card. EXTRACTION SUMMARY SIM ID Access Card created successfully ICCID: 8938003991816634752 IMSI: ADDITIONAL EXTRACTIONS FINISH 11. To end the process and return to the home screen, click Finish. Chapter 9: 113 ee

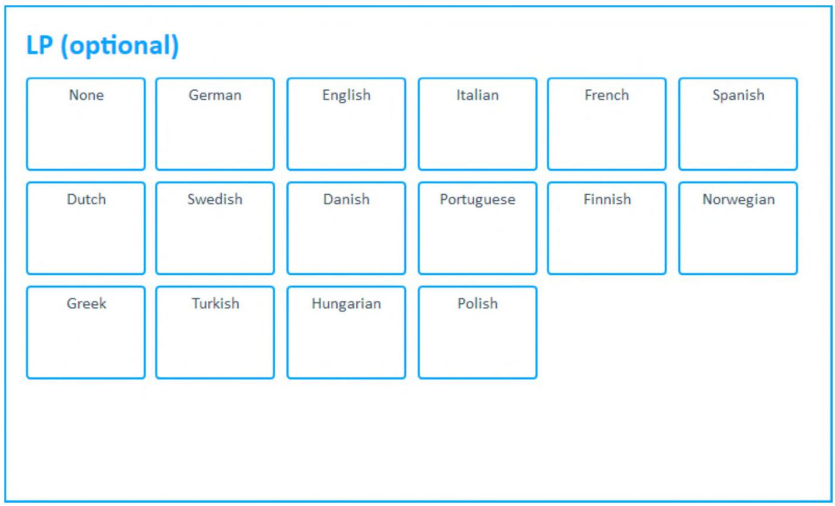


9.2.2. Entering SIM data manually 1. In the home screen, click Clone SIM. The Waiting for Device screen appears. 2. Insert the UFED SIM ID Access card. 3. Click Continue. The Select Source screen appears. Select Source Clone an Manually enter Create GSM existing SIM SIM data Test SIM card 4. Click Manually enter SIM data. The following screen appears. Source ICCID (1-20 digits) Enter ICCID fF Show Characters Cancel 5. Enter the SIM ICCID number (up to 20 digits). 6. Click OK. The following screen appears. 114

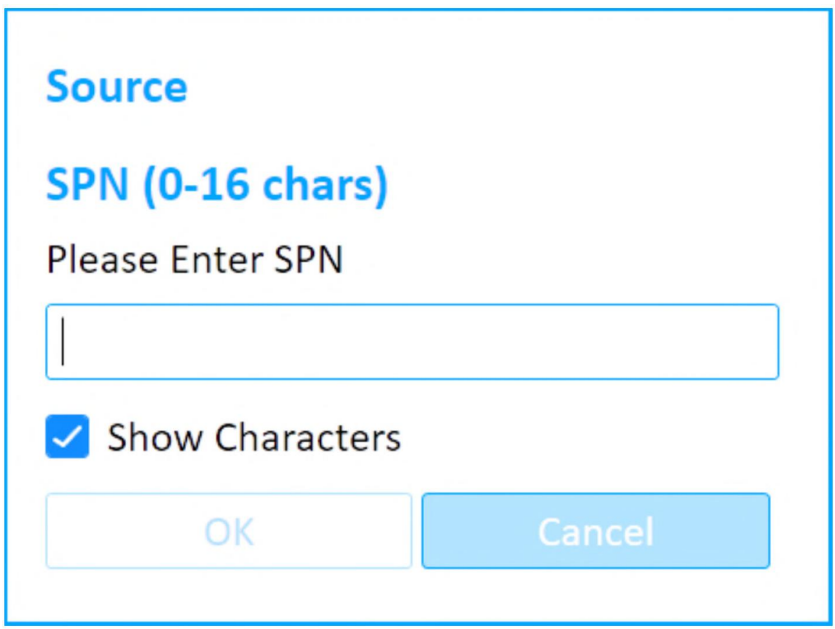


Source IMSI (1-15 digits) Enter IMSI Show Characters 7. Enter the SIM IMSI number [up to 15 digits], then click OK. -_ The Select Language screen appears. LP (optional) 8. If required, select either a language or click None. The Enter advanced settings screen appears. Chapter 9: 115 ee

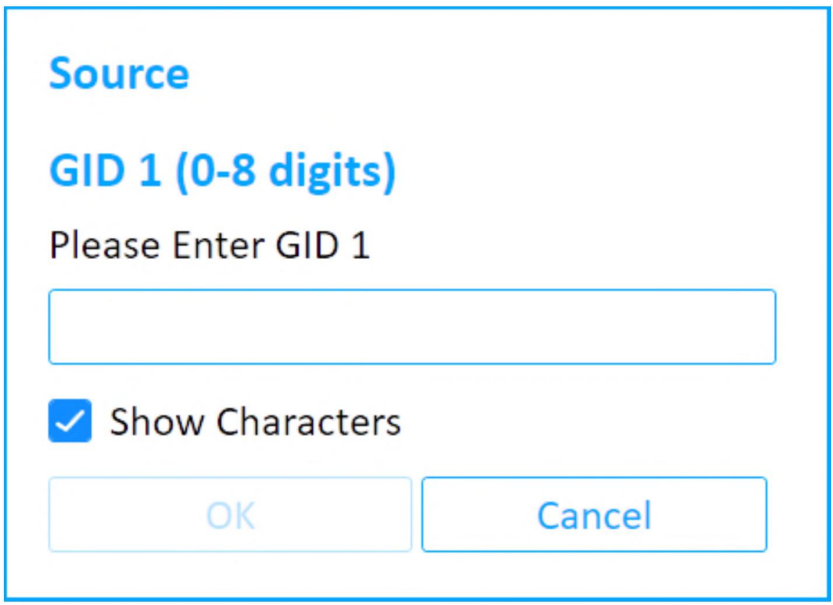




Enter advanced settings? Yes 9. Click No or Yes to continue. » Click No to continue. Proceed to step 15. » Click Yes to display the advanced settings. Extraction in Progress > Enter SPN screen appears. Source SPN (0-16 chars) Please Enter SPN Po Show Characters | Cancel 10. Enter the SIM SPN number [up to 16 digits], then click OK. The following screen appears. 116

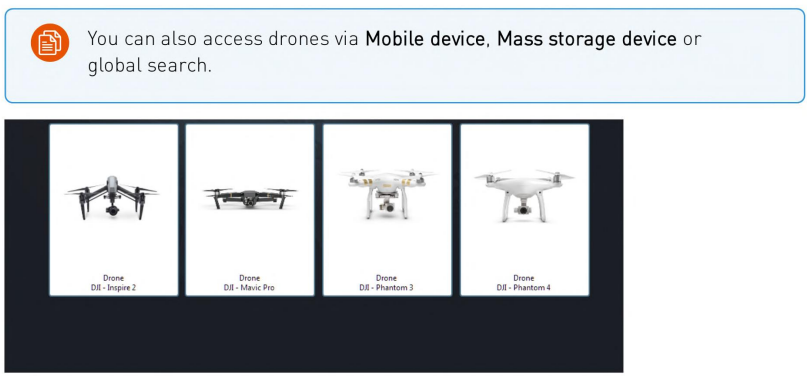


Source GID 1 (0-8 digits) Please Enter GID 1 pO Show Characters Cancel 11. Enter the SIM GID 1 number (up to 8 characters} and click OK. The Extraction in Progress > Enter GID 2 screen appears. 12. Enter the SIM GID 2 number [up to 8 characters). 13. Click OK. The Insert Target Card prompt appears. 14. Insert the UFED SIM ID access card Into . 15. Click Continue. The Extraction in Progress screen Is displayed throughout the data writing process. At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card. 16. To end the process and return to home screen click Finish. Chapter 9: 117

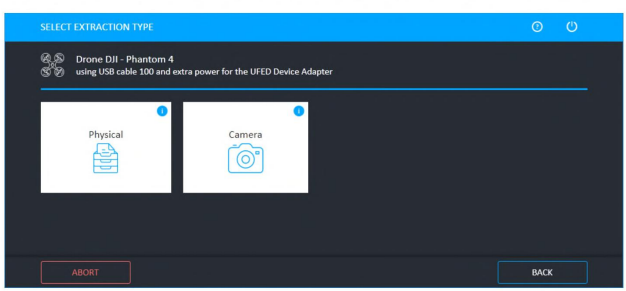


9.2.3. Creating a GSM test SIM 1. Click Clone SIM. The Waiting for Device screen appears. 2. Insert the SIM card into the SIM card reader slot located in the left of the front panel. 3. Click Continue. The Select Source screen appears. 4. Click Create GSM Test SIM. The following screen appears. Insert Target Card Insert SIM ID Access Card into the UFED Device Adapter with the SIM card's contacts facing down and the clipped corner pointing toward you. CONTINUE 5. Make sure that the target SIM card is inserted correctly into the SIM card reader slot, then click Continue. The Extraction in Progress screen Is displayed throughout the data reading process. At the end of the data writing process, a summary of the SIM cloning process is displayed, detailing the ICCID and IMSI information programmed to the SIM card. 6. To end the process and return to the home screen, click Finish. 118

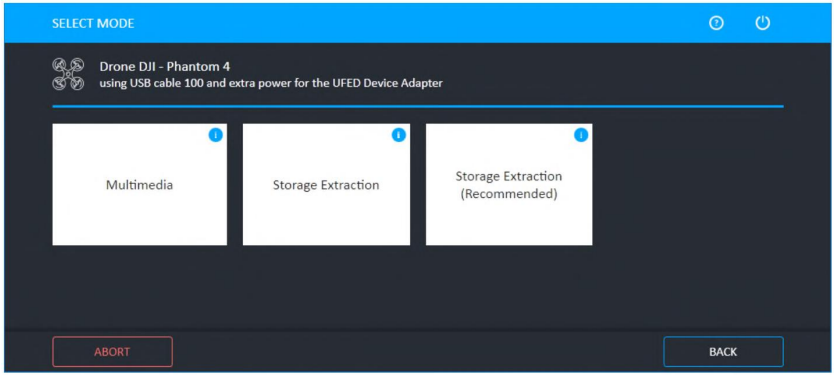
10. Drone extractions UFED enables you to extract flight data and multimedia files from supported drones. You can perform physical extractions, as well capture images of drones. For a complete list of Supported drones, refer to the UFED Supported Devices file in MyCellebrite. The following example shows how to perform a physical extraction of a drone. To perform a drone extraction: 1. Click Drone. The following window appears. You can also access drones via Mobile device, Mass storage device or global search. Drone DJI - Phantom 3 Physical Camera 3. Click Physical. The following window appears. Chapter 10: 119



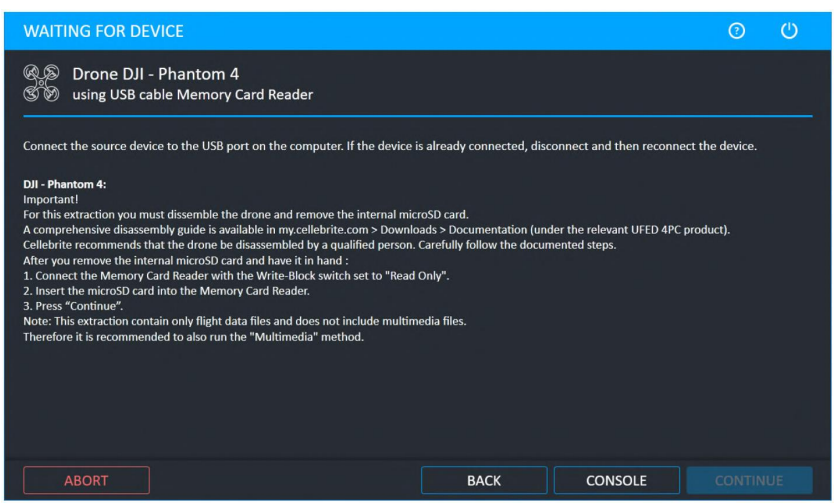
2. Select the required drone and then click **Next**. The following window appears.



SELECT MODE Drone DJ! - Phantom 4 using USB cable 100 and extra power for the UFED Device Adapter Storage Extraction Multimedia Storage Extraction 8 (Recommended) 4. Select an option as follows: > > > > > > Multimedia: The external microSD card stores the multimedia files of the drone i.e., (images and videos] only. To obtain a full data extraction including flight data, it is also recommended to run the “Storage Extraction Recommended” method. Storage Extraction: The internal microSD card stores the .dat file, which contains the flight data of the drone. The data stored on this card 1s updated to the time of the extraction. This extraction method Is easier than the Storage Extraction [Recommended] mode, but it requires the drone to be turned on which triggers additional log data that is written to the card. This extraction method already includes multimedia files, therefore the Multimedia mode is not required. Storage Extraction (Recommended): The internal microSD card stores the .dat file, which contains the flight data of the drone. The data stored on this card is updated to the time when the drone was last turned off. This is the recommended extraction method, because the drone stays off and no additional log data is written to the card. However this extraction method is more complicated due to the fact that the microSD card can only be accessed after disassembling the drone. This extraction method does not include multimedia files, therefore it is recommended to also run the Multimedia method. For information on disassembling the drone, refer to MyCellebrite.com. Cellebrite recommends that the drone be disassembled by a qualified person. Carefully follow the documented steps. For information on using optional timeframe and party filters, refer to the Overview Guide. The following window appears. 120

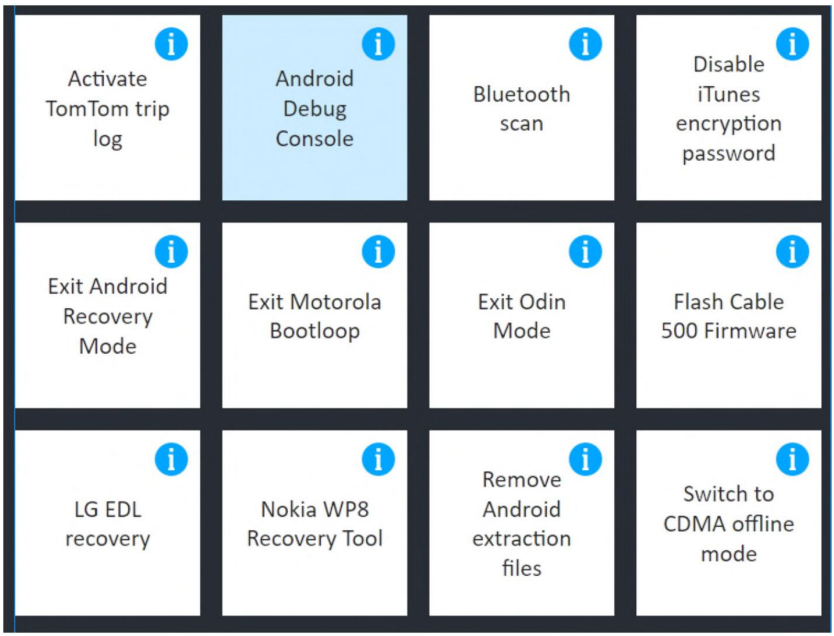

SELECT MODE
Drone DJI - Phantom 4
using USB cable 100 and extra power for the UFED Device Adapter
Multimedia
Storage Extraction
Storage Extraction (Recommended)
ABORT
BACK

WAITING FOR DEVICE ne DJI - Phantom 4 @W® using USB cable Memory Card Reader Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device. DJI - Phantom 4: Important! For this extraction you must dissemble the drone and remove the internal microSD card. A comprehensive disassembly guide is available in my.cellebrite.com > Downloads > Documentation (under the relevant UFED 4PC product). Cellebrite recommends that the drone be disassembled by a qualified person. Carefully follow the documented steps. After you remove the internal microSD card and have it in hand : 1. Connect the Memory Card Reader with the Write-Block switch set to "Read Only". 2. Insert the microSD card into the Memory Card Reader. 3. Press “Continue”. Note: This extraction contain only flight data files and does not include multimedia files. Therefore it is recommended to also run the "Multimedia" method. CONSOLE 5. Use the specified cable and follow the on-screen instructions. 6. Tap Continue. When the extraction completes, the Extraction completed successfully window appears. Chapter 10: 121


WAITING FOR DEVICE
Drone DJI - Phantom 4
using USB cable Memory Card Reader
Connect the source device to the USB port on the computer. If the device is already connected, disconnect and then reconnect the device.
DJI - Phantom 4:
Important!
For this extraction you must dissemble the drone and remove the internal microSD card.
A comprehensive disassembly guide is available in my.cellebrite.com > Downloads > Documentation (under the relevant UFED 4PC product).
Cellebrite recommends that the drone be disassembled by a qualified person. Carefully follow the documented steps.
After you remove the internal microSD card and have it in hand :
1. Connect the Memory Card Reader with the Write-Block switch set to "Read Only".
2. Insert the microSD card into the Memory Card Reader.
3. Press "Continue".
Note: This extraction contain only flight data files and does not include multimedia files.
Therefore it is recommended to also run the "Multimedia" method.
ABORT
BACK
CONSOLE
CONTINUE

The text on this page is estimated to be only 40.29% accurate

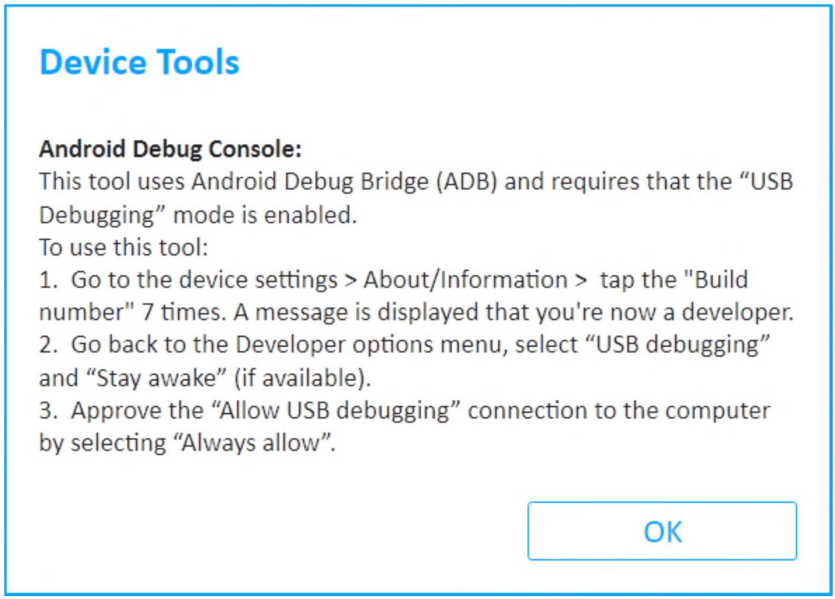
11. Device tools To access the device tools: » From the Home screen, click Device tools. The following window appears. Activate Android TomTom trip Debug log Console Disable Bluetooth iTunes scan encryption password Exit Android rece wat Exit Motorola Exit Odin Flash Cable — Bootloop Mode 500 Firmware Switch to CDMA offline mode Remove LG EDL Nokia WP8 Android recovery Recovery Tool extraction files The Device Tools screen provides access to the following tools: TL CUI ee TOG UNNI cad oat ert eh ier hts eet ls eta ahs tae 124 iieZ. Ancol IDEDWG CONSOLE: 22 us2 sei ch adie da Sisekeeenescededdiiastedctie shel s Diskiscinihiwees icededialdes 124 Migs ey MOG a IN gia aes decedent ate es eal d fasta aloo cae de ren, cee Sod nee 126 1A. Disable i Uunes-Aneryptiont PaSSWOPd oo .ots eee t soc cwuy te tywokueyadewestendeduadieewesedegeeduus 126 1 EXICAMOPOIG FECOVERY INOUE otis sce ce loti y ak ile Leeyoan Vole val ieaee Reise bed, 127 aes RO honG iat OU UIOD IG .ccangooakscedd tartan en kbeteeapedatabee tlie ore eeaeeedat 127 oy EMME CICMMIMNOU Es. 255.22. cecesaes nec ueieie ise ies bouecoteL estes coca cs ut heats esdetca ia: 127 6. Flash Caple S00 PIntMWar: cocci gupta otek eel eoe ue ebecus seul als peptar yl Lee aa 127 ree alee Ni WOU ipa tcl dee eae need Ate ease a hea nodal ia beeen ena a 2h Spite Secclan anes, 128 LU Nokia WPS TeCOvery TOO 2.214.064 MilepreeddodasenlLvidlidoesenvadsciedaelbuddteasedesrdcauel 128 122


Activate TomTom trip log
Android Debug Console
Bluetooth scan
Disable iTunes encryption password
Exit Android Recovery Mode
Exit Motorola Bootloop
Exit Odin Mode
Flash Cable 500 Firmware
LG EDL recovery
Nokia WP8 Recovery Tool
Remove Android extraction files
Switch to CDMA offline mode

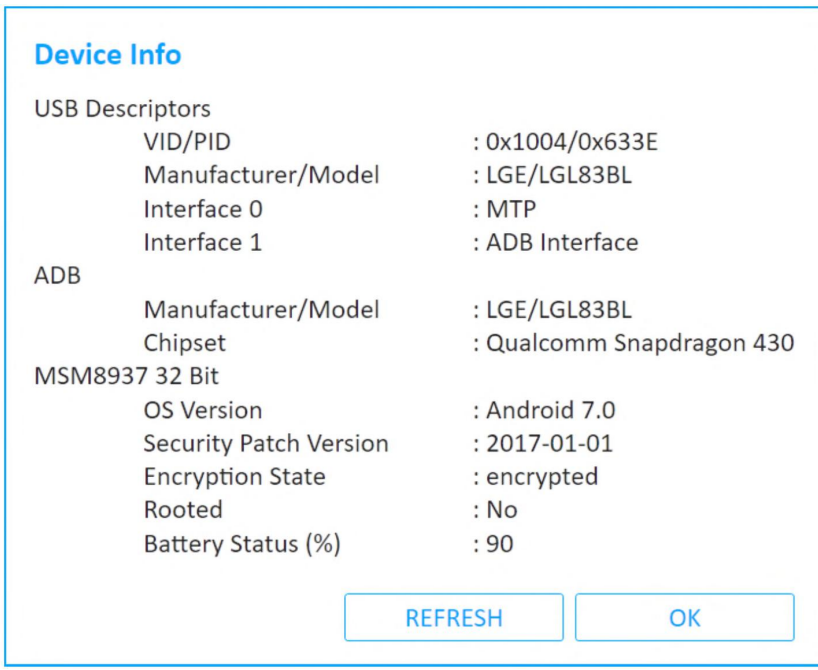
The text on this page is estimated to be only 23.65% accurate

ThA1. Remove Android @xtract Ory WES ico oes eaite ied Sa dee weeumeeie Sad adue views een gen eee 128 a |. eSNG) EX VNOS ROCOVEI Yc taht cineca nu sta edu duets badeuee tale psbelasadonr Ga vence sauce 128 Tis13. Saved APKs trom APKGOWMGRade 226 occ ck ee ese cee ca eee oda cvew ee adnasauus 129 VieideSwiten to CDMA, OMe TOU asco ear ae yg ceed ela nant cen ukeetesiey coe eued 130 5. Uninstall Windows mobile client ...2.. 0.0.20. o eee eee eee eee eee 131 Chapter 11: 13

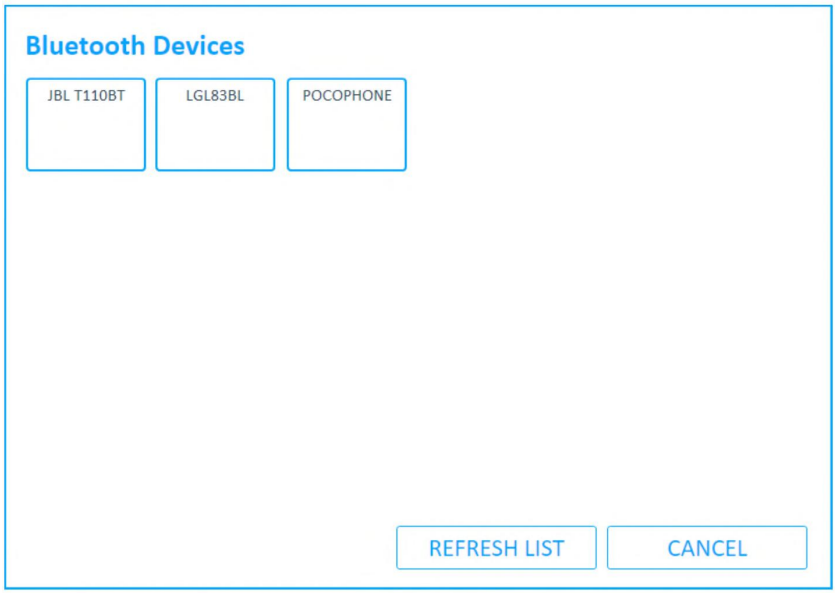
11.1. Activate TomTom trip log This tool enables you to activate or deactivate the trip log logging feature of a connected TomTom device, which Is often disabled by the user To Activate TomTom trip log: 1. Click Tools and then click Activate TomTom trip log. The Select Mode prompt appears. 2. Select the desired mode. A prompt labeled Attention appears requesting to connect the device to Cellebrite UFED. 3. Connect the device to Cellebrite UFED. 4. Click Continue. 11.2. Android Debug Console This tool retrieves device information using Android Debug Bridge [ADB]. To use the tool: 1. Click Tools and then click Android Debug Console. 2. If required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port [4PC and non-kiosk platforms only]. The following window appears. Device Tools Android Debug Console: This tool uses Android Debug Bridge (ADB) and requires that the “USB Debugging” mode is enabled. To use this tool: 1. Go to the device settings > About/Information > tap the "Build number" 7 times. A message is displayed that you're now a developer. 2. Go back to the Developer options menu, select “USB debugging” and “Stay awake” (if available). 3. Approve the “Allow USB debugging” connection to the computer by selecting “Always allow”. 3. Follow the on-screen instructions. 4. Tap OKto receive the device information. The following window appears. 124


Device Tools
Android Debug Console:
This tool uses Android Debug Bridge (ADB) and requires that the “USB Debugging” mode is enabled.
To use this tool:
1. Go to the device settings > About/Information > tap the "Build number" 7 times. A message is displayed that you're now a developer.
2. Go back to the Developer options menu, select “USB debugging” and “Stay awake” (if available).
3. Approve the “Allow USB debugging” connection to the computer by selecting “Always allow”.
OK

Device Info USB Descriptors VID/PID Manufacturer/Model Interface O Interface 1 Manufacturer/Model Chipset MSM8937 32 Bit Chapter 11: OS Version Security Patch Version Encryption State Rooted Battery Status (%) : 0x1004/0x633E : LGE/LGL83BL : MTP : ADB Interface : LGE/LGL83BL : Qualcomm Snapdragon 430 : Android 7.0 : 2017-01-01 : encrypted :No :90 REFRESH | 129



11.3. Bluetooth scan This tool enables you to scan for available Bluetooth devices in your proximity and to pair with them. Make sure that Bluetooth is enabled on the device. To perform a Bluetooth scan: 1. Click tools and then click Bluetooth scan. 2. Connect the Cellebrite UFED Device Adapter [4PC and non-kiosk platforms only). 3. Alist of Bluetooth devices in the vicinity appears. Select one or the following options: » Click one of the devices: The Device summary window appears. » Click Continue: Device summary window appears » Click Refresh list: Device tool in progress window appears and tries to find additional devices. Bluetooth Devices JBL T110BT LGL83BL POCOPHONE | REFRESH LIST || CANCEL 11.4. Disable iTunes encryption password If you select to enable backup encryption during an iOS File system extraction (Full or Backup modes], and for any reason the extraction was stopped in the middle, the device may remain encrypted. This option resets the encryption on the device. 126

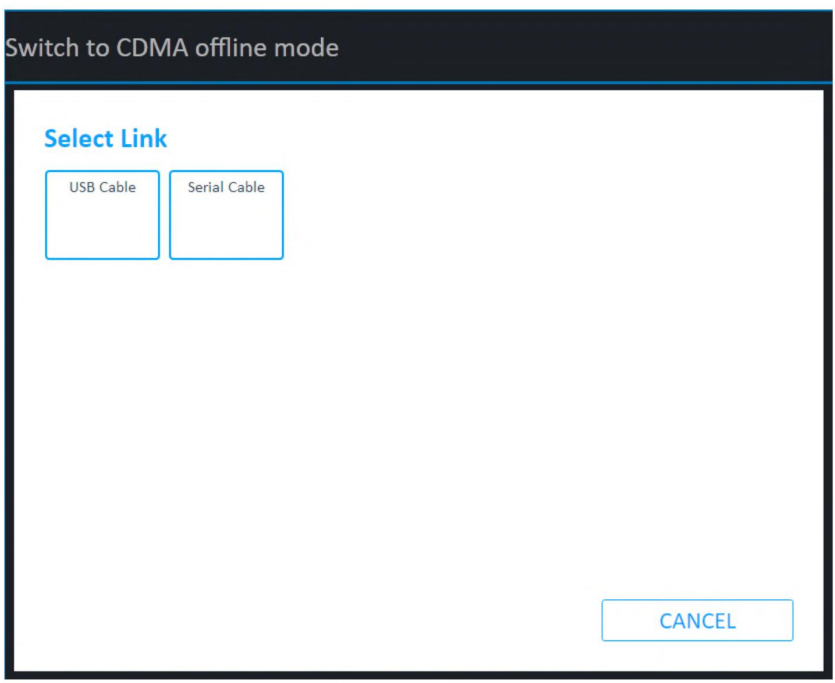


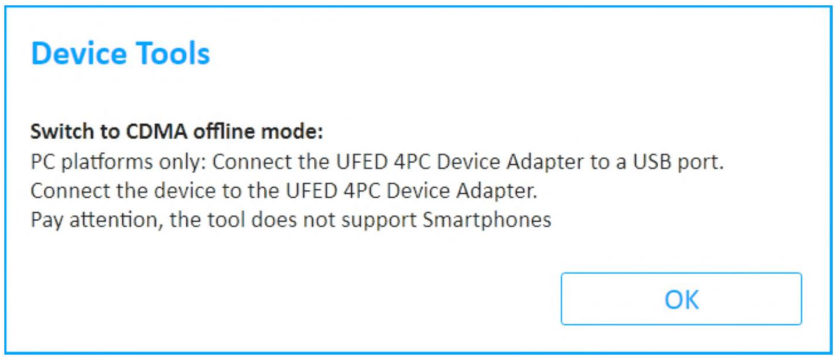
11.5. Exit Android recovery mode This tool includes two options related to physical extractions using the Forensic Recovery Partition method on Android devices. » Exit recovery mode: In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode. >» Exit bootloop: In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop. 11.6. Exit Motorola Bootloop In Some cases, due to device failure, or if the Motorola mobile device was improperly disconnected from Cellebrite UFED, the mobile device keeps rebooting instead of entering the normal mode. This option enables the device to be taken out of this bootloop. 11.7. Exit Odin mode To perform physical extractions on some Samsung devices, the device is placed in Odin mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from , the mobile device remains in Odin mode. This option enables the device to be taken out of Odin mode. 11.8. Flash Cable 500 Firmware When using the Smart ADB method, the firmware on Cable No. 500 is changed and will no longer support the Cellebrite UFED User Lock Code Recovery Tool. The Flash Cable 500 Firmware tool flashes the required firmware to the cable to support either the Smart ADB method or the Cellebrite UFED User Lock Code Recovery Tool. © In the Smart ADB method, Cellebrite UFED verifies the cable firmware and flashes it if required. Cellebrite UFED User Lock Code Recovery Tool does not include cable verification. To flash the firmware for the Smart ADB extraction method: 1. Click Tools and then click Flash Cable 500 Firmware. 2. Connect the Cellebrite UFED Device Adapter to a USB port [4PC and non-kiosk platforms only). Chapter 11: IZ? Le

3. Connect Cable No. 500 (side A) to the USB port. 4. Tap Smart ADB Firmware and wait for the process to finish. 11.9. LG EDL recovery In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the LG device remains in emergency download [EDL] mode and appears off. This option enables the device to be taken out of EDL mode. To use the tool: 1. Click Tools and then click LG EDL recovery. 2. lf required, you will be prompted to connect the Cellebrite UFED Device Adapter to a USB port [4PC and non-kiosk platforms only). 3. Follow the on-screen instructions. 4. Tap Continue and wait for the tool to finish running. 11.10. Nokia WP8 recovery tool To perform physical extraction on some Nokia Windows Phone 8 devices, the device is placed in recovery mode. In some cases, due to device failure, or if the mobile device was improperly disconnected from , the mobile device remains in recovery mode. This option enables the device to be taken out of recovery mode. 11.11. Remove Android extraction files When performing extractions of devices with Android operating systems, a client Is installed and some files are written to the mobile device. In some cases [e.g., due to a failure, or if the mobile device was improperly disconnected from] the client and the files remain on the mobile device. This tool uninstalls the client and removes the files from the device. 11.12. Samsung Exynos Recovery In some cases, due to device failure, or if the mobile device was improperly disconnected from Cellebrite UFED, the device remains off and the Android OS does not start. This option attempts to resolve this issue. 128

11.13. Saved APKs from APK downgrade This tool saves APKs that could not be reinstalled on the device during an APK downgrade extraction. An example is displayed next. APKs from APK downgrade | Device | Extraction date L | SM-A7SOFN Galaxy A7 (2018) duos 7/15/2019 7:11:41 PM Select the devices and the location to save the APKs To save the APK: 1. Select the device. 2. Select the location where the APK should be saved. 3. Click Save. Chapter 11: 129

11.14. Switch to CDMA offline mode This tool enables you to switch radio on CDMA devices to offline mode. To switch to CDMA offline mode: 1. Click tools and then click Switch to CDMA offline mode. 2. Connect the Cellebrite UFED Device Adapter [4PC and non-kiosk platforms only]. The Select Link prompt appears. Switch to CDMA offline mode Select Link USB Cable Serial Cable CANCEL 3. Select the link type (USB Cable or Serial Cable}. The Device Tool in Progress window appears. Device Tools Switch to CDMA offline mode: PC platforms only: Connect the UFED 4PC Device Adapter to a USB port. Connect the device to the UFED 4PC Device Adapter. Pay attention, the tool does not support Smartphones OK 4. Tap OK. Upon completion, the Device Tool Summary appears. 130




Device Tools
Switch to CDMA offline mode:
PC platforms only: Connect the UFED 4PC Device Adapter to a USB port.
Connect the device to the UFED 4PC Device Adapter.
Pay attention, the tool does not support Smartphones
OK

11.15. Uninstall Windows mobile client To perform logical extractions on devices with Windows Phone operating systems, a client is installed on the device. In some cases, due to a device failure, or if the mobile device was improperly disconnected from , the client remains installed on the mobile device. This option enables the client to be manually uninstalled. Chapter 11: 134

12. Glossary C CAS Cellebrite Advanced Services (CAS] offers customers the ability to recover valuable evidence from heavily damaged, locked or encrypted devices. Cellebrite UFED 4PC Enables users to deploy extraction capabilities on Windows based tablets, laptops, and desktop computer systems. It performs physical, logical, file system and password extractions on a wide range of devices. Cellebrite UFED Touch Enables the simplified extraction of mobile device data. Depending on the license purchased, it performs physical, logical, file system and password extractions ona wide range of devices. P Physical/Logical Analyzer An analysis and reporting tool for logical, file system and physical extractions. This software solution provides users with the capability to extract data, perform advanced analysis, decoding and reporting and presenting the results in a clear and concise manner. U UFED Universal Forensic Extraction Device haz Chapter 12: Glossary

Accessories 10 ADB, definition 60 Android backup 41, 44-45, 50 Android backup APK downgrade 45, 50 APK downgrade 45, 50 B Bluetooth scan 126 Bluetooth, logical extraction 24 Boot Loader, definition 60 C Capture 9, 95, 101-102 Capture images 9, 95-96, 119 Capture images and screenshots 10, qs Cellebrite YouTube channel 14 Clone SIM 9, 107, 111-112, 114, 118 Cloning an existing SIM card ID 111 D Device tools 122 Drone, extractions 119 EB Entering SIM data manually 114 Exit Motorola bootloop 127 Extracted passwords folder 32 Extracted SIM data folder 110 Extraction in progress 30, 40, 61, 64, 84, 90, 113, 116, 118 Extractions, (Refer to Performing extractions in MyCellebrite) 9, 16, 32 F File system extraction 9, 38, 107, 126 File system extraction folder 40 Files, logical extraction type 22 Flashing 82 Forensic recovery partition 87 FW flashing 82 GSM test SIM 118 H Help 15 Home screen 32, 66, 73, 122 | iOS extraction 17 iTunes backup encryption 20 J JTAG 45 Legal notices 2 133

Logical extraction 7, 9-10, 14-17, 20- Settings 41, 66 21, 24, 107 N SIM data extraction 107, 110 SIM extraction 9 Nokia WP8 recovery tool 128 0 Smart ADB method, tool 127 Odin mode 127 Specifications 2, 12 Overview 7, 12, 17, 21, 38, 41, 46, 50, Specify a network location 93, 120 56, 60, 63, 66, 82, 85, 88, 91, 120 Supported devices 14 p Switch to CDMA offline mode 130 Password extraction 9, 29 System requirements 8 U Performing a file system extraction 38 Performing a physical extraction 60 UFED Device Adapter 11, 13, 124, 126Performing extractions 1 128, 130 UFED User Lock Code Recovery Tool 127 Performing SIM data extraction 107 Physical extraction 9, 56, 59-60, 62-63, 65, 82, 85, 87, 128 Unallocated space 9 Q Using cables and tips 13 Qualcomm chipsets 85 Ww R Working with TomTom 124 Re-enable User Lock option 33 Rooted Android devices, physical extraction 63 S Samsung Exynos Recovery 128 Screenshots 10, 95, 100, 103 Select content types 14 Select extraction location 82 134 2" Cellebrite es